NDIA Systems Engineering Conference 2001

Managing Vulnerabilities in Your Networked Systems Using an Industry Standards Effort

Robert A. Martin
The MITRE Corporation

25 October 2001

The views expressed in this presentation are those of the authors and do not necessarily reflect the policies or position of The MITRE Corporation.

Outline

➡ **Background and Motivation**

0 **Finding Out About Vulnerabilities**

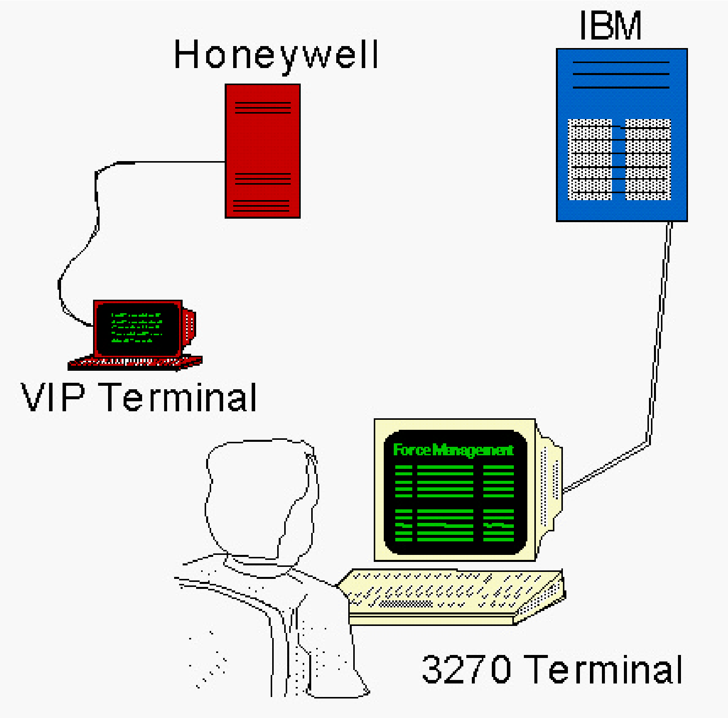
0 **The Problem and a Solution - CVE**

0 **CVE Compatibility**

0 **The CVE Process**

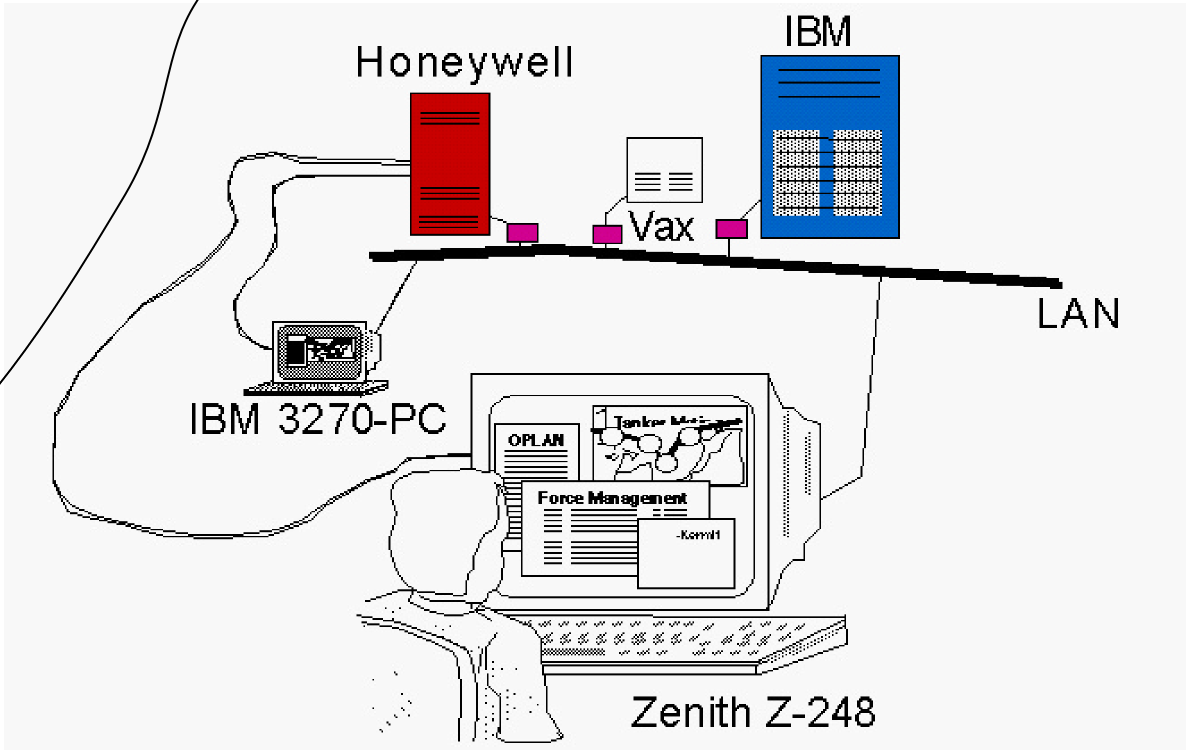
0 **Summary**

DoD started w/stand-alone computers, terminals & custom S/W -- Then came PCs w/COTS S/W terminal emulators and TCP/IP LANs



mid-70’s Mainframes with direct wired “Terminals”

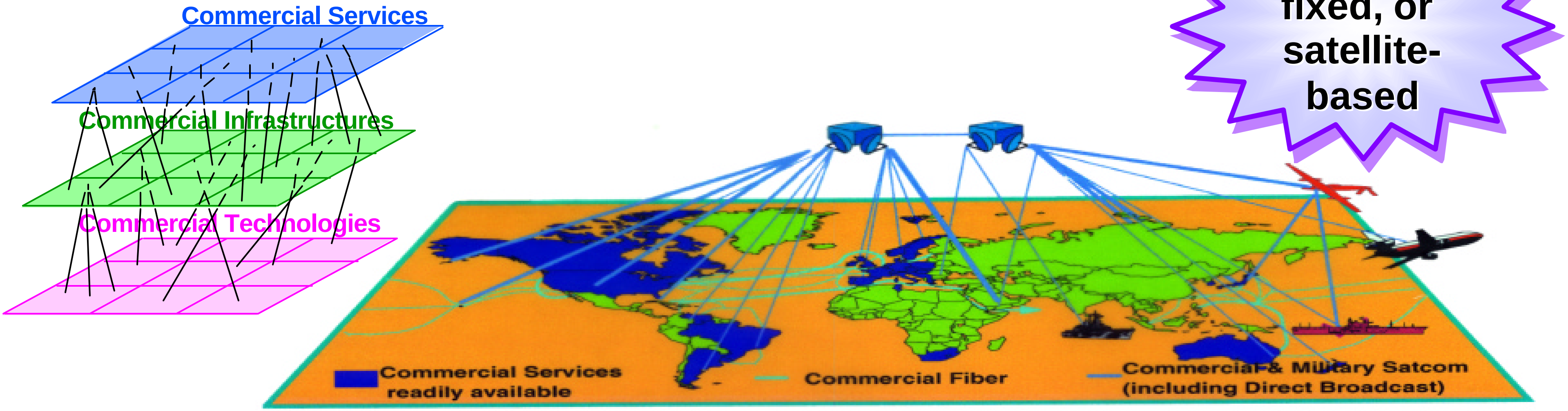
mid-80’s Mainframes
w/BIU interfaced “TCP/IP LAN”
w/PC-based “Terminal Emulators”

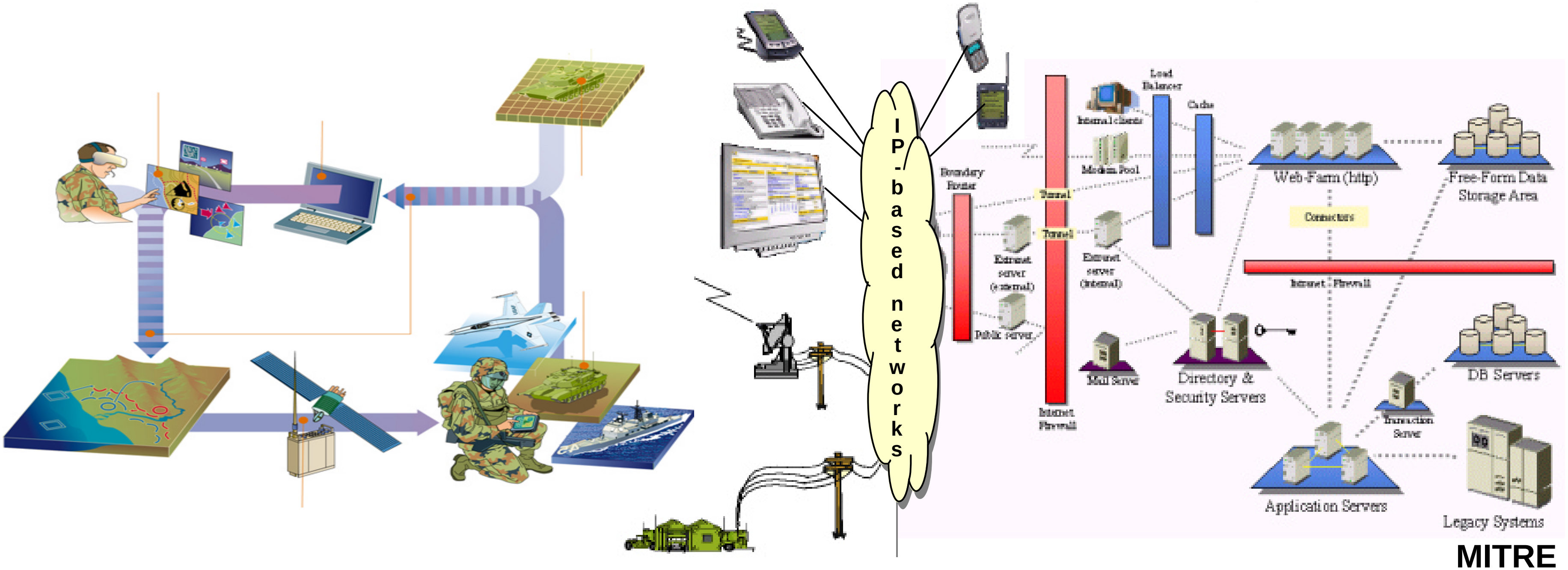


BIU - Bus Interface Units

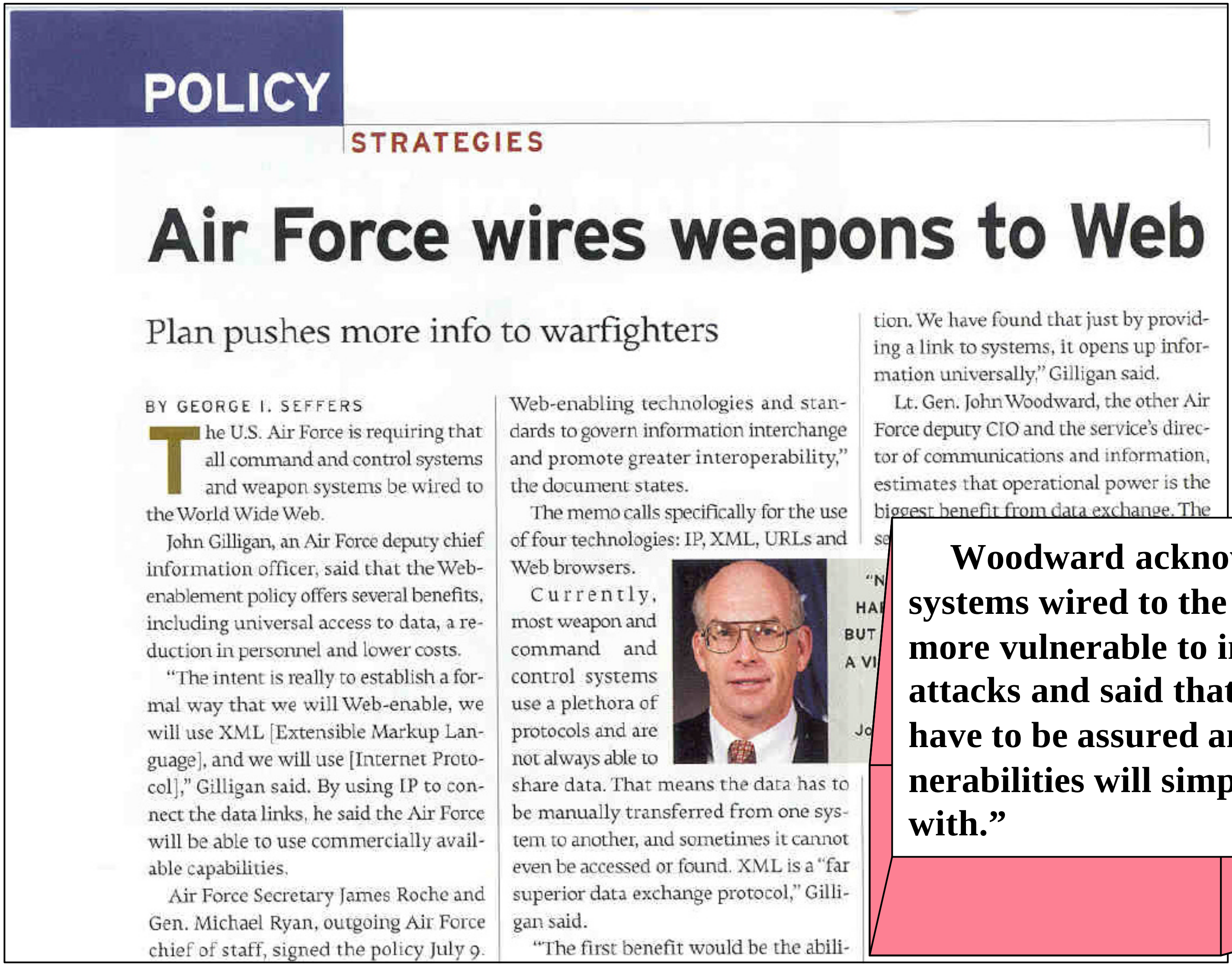
Now systems are being built using commercial products & S/W and connected within IP-based networks

wireless, fixed, or satellite-based


Commercial Services
Commercial Infrastructures
Commercial Technologies
Commercial Services readily available
Commercial Fiber
Commercial & Military Satcom (including Direct Broadcast)



DoD's Move to IP will Leverage Commercially Available Capabilities… and Liabilities….



POLICY

STRATEGIES

Air Force wires weapons to Web

Plan pushes more info to warfighters

BY GEORGE I. SEFFERS

The U.S. Air Force is requiring that all command and control systems and weapon systems be wired to the World Wide Web.

John Gilligan, an Air Force deputy chief information officer, said that the Web-enablement policy offers several benefits, including universal access to data, a reduction in personnel and lower costs.

"The intent is really to establish a formal way that we will Web-enable, we will use XML [Extensible Markup Language], and we will use [Internet Protocol]," Gilligan said. By using IP to connect the data links, he said the Air Force will be able to use commercially available capabilities.

Air Force Secretary James Roche and Gen. Michael Ryan, outgoing Air Force chief of staff, signed the policy July 9.

Web-enabling technologies and standards to govern information interchange and promote greater interoperability," the document states.

The memo calls specifically for the use of four technologies: IP, XML, URLs and Web browsers.

Currently, most weapon and command and control systems use a plethora of protocols and are not always able to share data. That means the data has to be manually transferred from one system to another, and sometimes it cannot even be accessed or found. XML is a "far superior data exchange protocol," Gilligan said.

"The first benefit would be the ability

tion. We have found that just by providing a link to systems, it opens up information universally," Gilligan said.

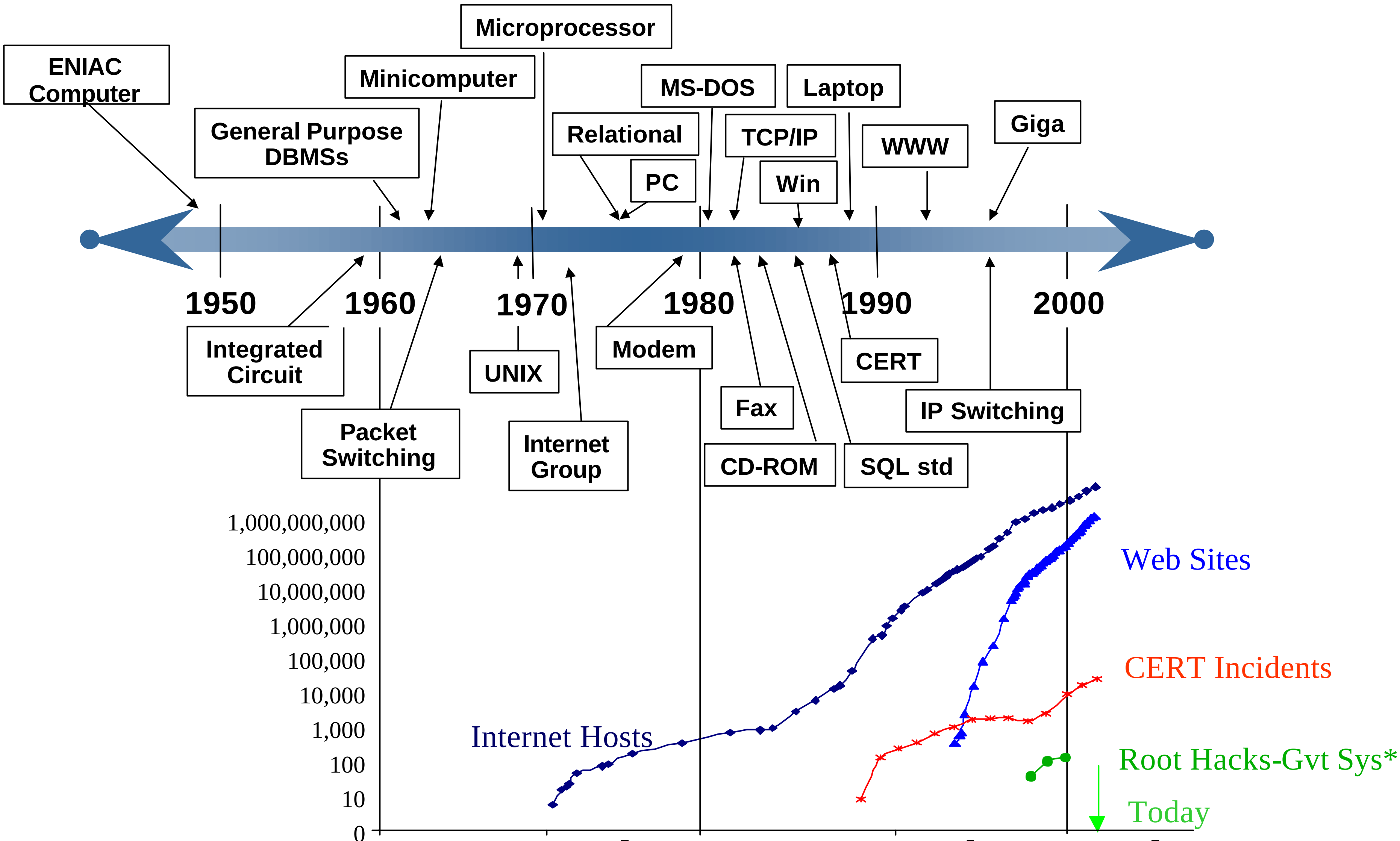
Lt. Gen. John Woodward, the other Air Force deputy CIO and the service's director of communications and information, estimates that operational power is the biggest benefit from data exchange. The se

"N
HA
BUT
A VI
Jo

Woodward acknowledged that weapon systems wired to the Web will be even more vulnerable to information warfare attacks and said that information will have to be assured and additional vulnerabilities will simply have "to be dealt with."

Federal Computer Week, 10 September 2001, page 46

The explosive growth of commercial technology and the Internet has taken us all for a ride…

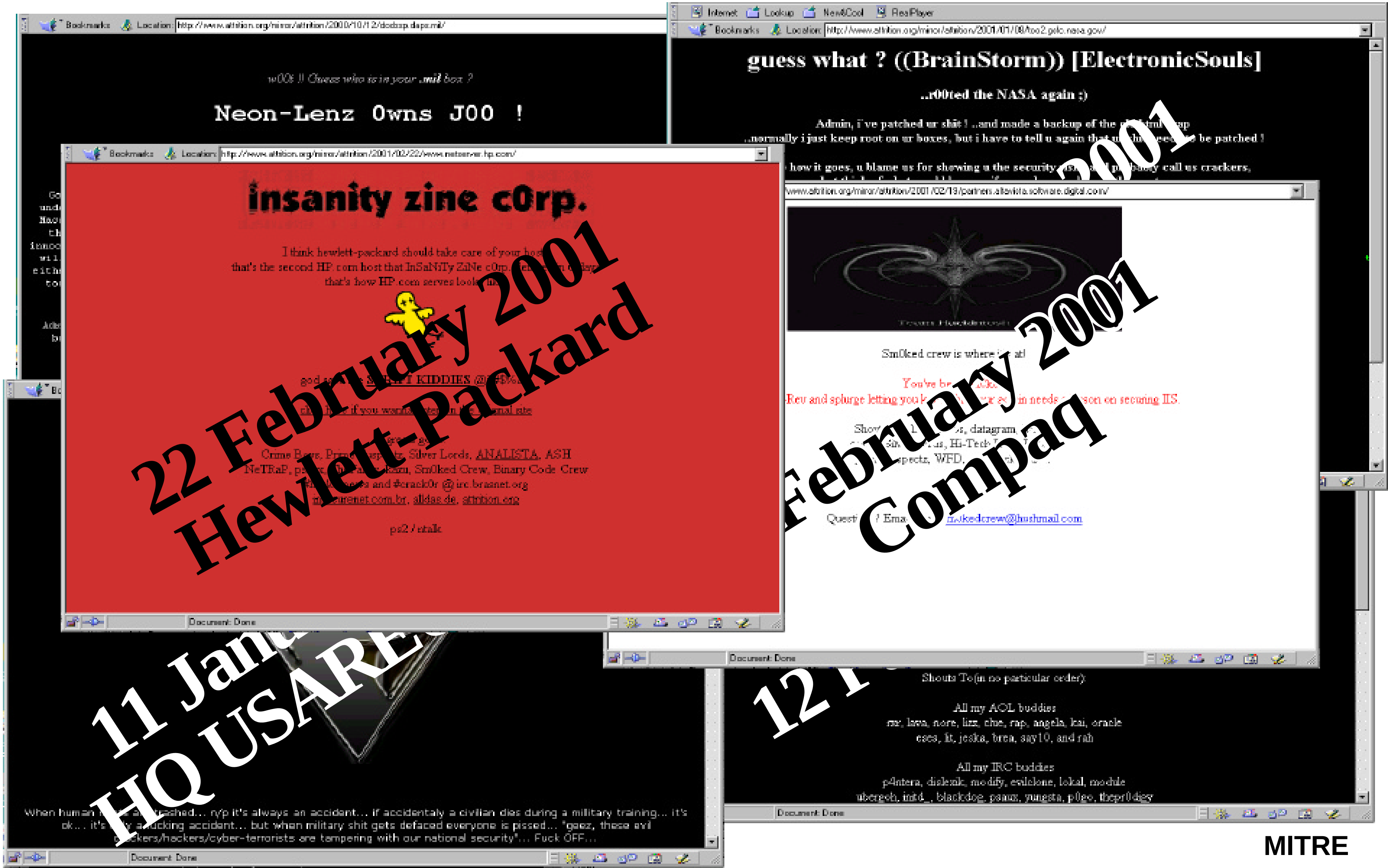


and sometimes it's a bumpy ride.

MITRE

*GSA congressional testimony 4/5/01

Organization’s Internet-visible “Faces” are being abused through Vulnerabilities in Commercial S/W



Location: http://www.attrition.org/mirror/attrition/2000/10/12/dodssp.daps.mil/

w00t !! Guess who is in your .mil box ?

Neon-Lenz Owns J00 !

Location: http://www.attrition.org/mirror/attrition/2001/01/09/too2.gsfc.nasa.gov/

guess what ? ((BrainStorm)) [ElectronicSouls]

..r00ted the NASA again ;)

Admin, i've patched ur shit ! ..and made a backup of the old html ..ap
..normally i just keep root on ur boxes, but i have to tell u again that ur shi... need.. to be patched !

... how it goes, u blame us for showing u the security ris... and pr... bably call us crackers,

Location: http://www.attrition.org/mirror/attrition/2001/02/22/www.netserver.hp.com/

insanity zine c0rp.

I think hewlett-packard should take care of your host
that's the second HP com host that InSaNiTy ZiNe c0rp. ...
that's how HP com serves look...

god ... SCRIPT KIDDIES @#$%...

click here if you wanna ... ternal site

Crime Boys, Prime ... Silver Lords, ANALISTA, ASH
NeTRaP, p... Sm0ked Crew, Binary Code Crew
... and #crack0r @ irc.brasnet.org
... net.com.br, alldas.de, attrition.org

ps2 / ntalk

Document: Done

www.attrition.org/mirror/attrition/2001/02/19/partners.altavista.software.digital.com/

Sm0ked crew is where ... at!

You've be... ...cked

Rev and splurge letting you k... ... in needs ... son on securing IIS.

Show... datagram, ...
... Hi-Tech ...
... pectz, WFD, ...

Questi... / Ema... sm0kedcrew@hushmail.com

Document: Done

Shouts To(in no particular order):

All my AOL buddies
rsr, lava, nore, lizz, clue, rap, angela, kai, oracle
esea, lt, jeska, brea, say10, and rah

All my IRC buddies
p4ntera, dislexik, modify, evilclone, lokal, module
ubergeek, intd_, blackdoe, psaux, yungsta, p0lgo, thepr0digy

Document: Done

When human ... trashed... n/p it's always an accident... if accidentaly a civilian dies during a military training... it's ok... it's ... accident... but when military shit gets defaced everyone is pissed... "geez, these evil ...ckers/hackers/cyber-terrorists are tampering with our national security"... Fuck OFF...

Document: Done

22 February 2001
Hewlett-Packard

... February 2001
Compaq

... 2001

11 Jan...
HQ USAREU...

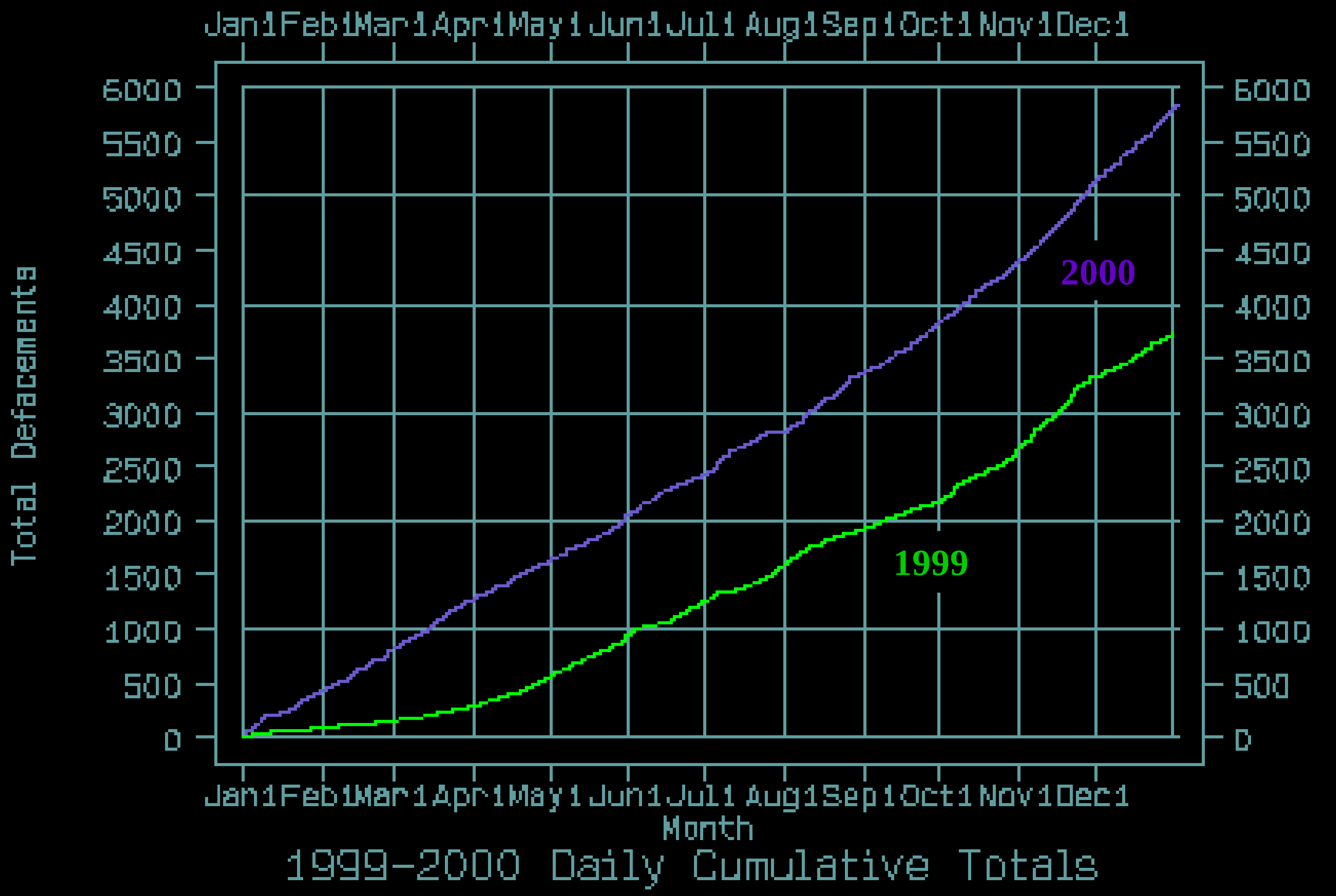
12 F...

MITRE

The Wrong Publicity Can Be Bad...

"BIG DEAL, KYLE. WHO **HASN'T** HACKED INTO MICROSOFT?"

1999 vs. 2000 Daily Hack Cumulative Total Comparison



Source: Attrition.org

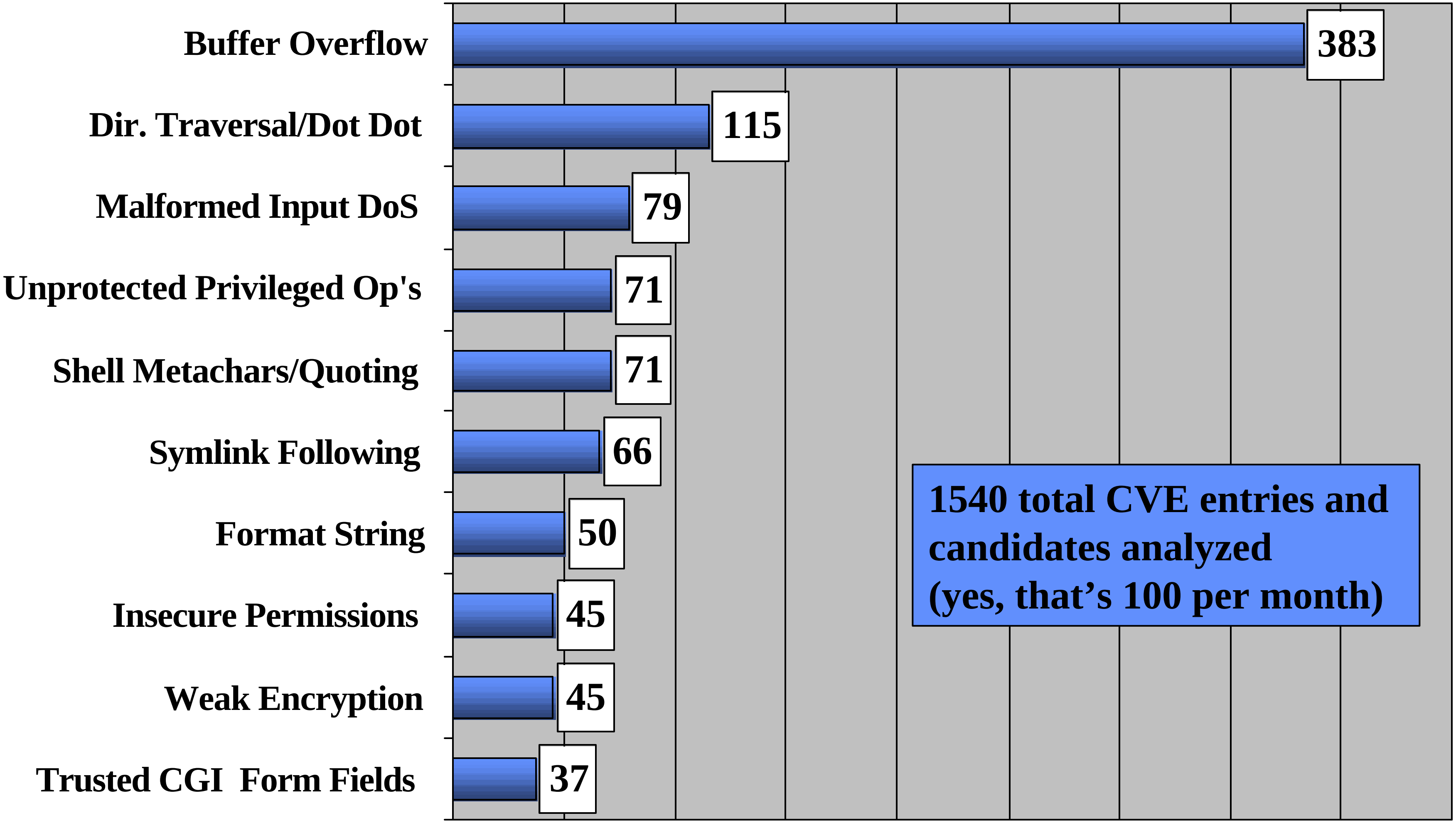
MITRE

Software problems with security implications are referred to as Vulnerabilities or Exposures

- Vulnerabilities are security related software problems that could directly allow serious damage
- Examples:
  - phf, ToolTalk, Smurf, rpc.cmsd, etc.
  - Oracle XSQL servlet 1.0.3.0 and earlier allows remote attackers to execute arbitrary Java code by redirecting the XSQL server to another source via the xml-stylesheet parameter in the xslt stylesheet. *[9 Jan 01 Georgi Guninski]*

- Exposures are security related software problems that could be used as stepping stones for a successful attack
- Examples:
  - Running finger, poor logging practices, etc.

Top Ten Vulnerability Types in CVE (Issues publicized between Jan 2000 and April 2001)



1540 total CVE entries and candidates analyzed
(yes, that’s 100 per month)

Vulnerabilities Have Been Found in Almost Every Type of Commercial Software There Is

Mail Servers

- 1st Up Mail Server
- All-Mail
- ALMail32
- Avirt Mail Server
- Becky! Internet Mail
- CWMail
- Domino Mail Server
- Exchange Server
- Hotmail
- Internet Anywhere Mail Server
- ITHouse Mail Server
- Microsoft Exchange
- Pegasus Mail
- Sendmail

Security Software

- ACE/Server
- BlackICE Agent
- BlackICE Defender
- Certificate Server
- CProxy Server
- ETrust Intrusion Detection
- GateKeeper
- InterScan VirusWall
- Kerberos 5
- Norton AntiVirus
- PGP
- SiteMinder
- Tripwire

Web servers & tools

- Domino HTTP Server
- IIS
- NCSA Web Server
- Sawmill
- WebTrends Log Analyzer

Internet

- AFS
- Apache
- BIND
- CGI
- Cron
- IMAP

Routers

- 3220-H DSL Router
- 650-ST ISDN Router
- Ascend Routers
- Cisco Routers
- R-series routers

Network Applications

- BackOffice
- Meeting Maker
- NetMeeting

DBMSs

- Access
- DB2 Universal Database
- FileMaker Pro
- MSQL
- Oracle

Desktop Applications

- Acrobat
- Clip Art
- Excel
- FrameMaker
- Internet Explorer
- Napster client
- Notes Client
- Novell client
- Office
- Outlook
- PowerPoint
- Project
- Quake
- R5 Client
- StarOffice
- Timbuktu Pro
- Word
- Works
- Workshop

Development Tools

- ClearCase
- ColdFusion
- Flash
- Frontpage
- GNU Emacs
- JRun
- WebLogic Server
- Visual Basic
- Visual Studio

Operating Systems

- AIX
- BeOS
- BSD/OS
- DG/UX
- FreeBSD
- HP-UX
- IRIX
- Linux
- MacOS Runtime for Java
- MPE/iX
- NetWare
- OpenBSD
- Palm OS
- Red Hat
- Security-Enhanced Linux
- Solaris
- SunOS
- Ultrix
- Windows 2000
- Windows 95
- Windows 98
- Windows ME
- Windows NT

Firewalls

- Firewall-1
- Gauntlet Firewall
- PIX Firewall
- Raptor Firewall
- SOHO Firewall

Sample of Vulnerabilities Announced in 1999 & 2000

Outline

0 **Background and Motivation**

➡ **Finding Out About Vulnerabilities**

0 **The Problem and a Solution - CVE**

0 **CVE Compatibility**

0 **The CVE Process**

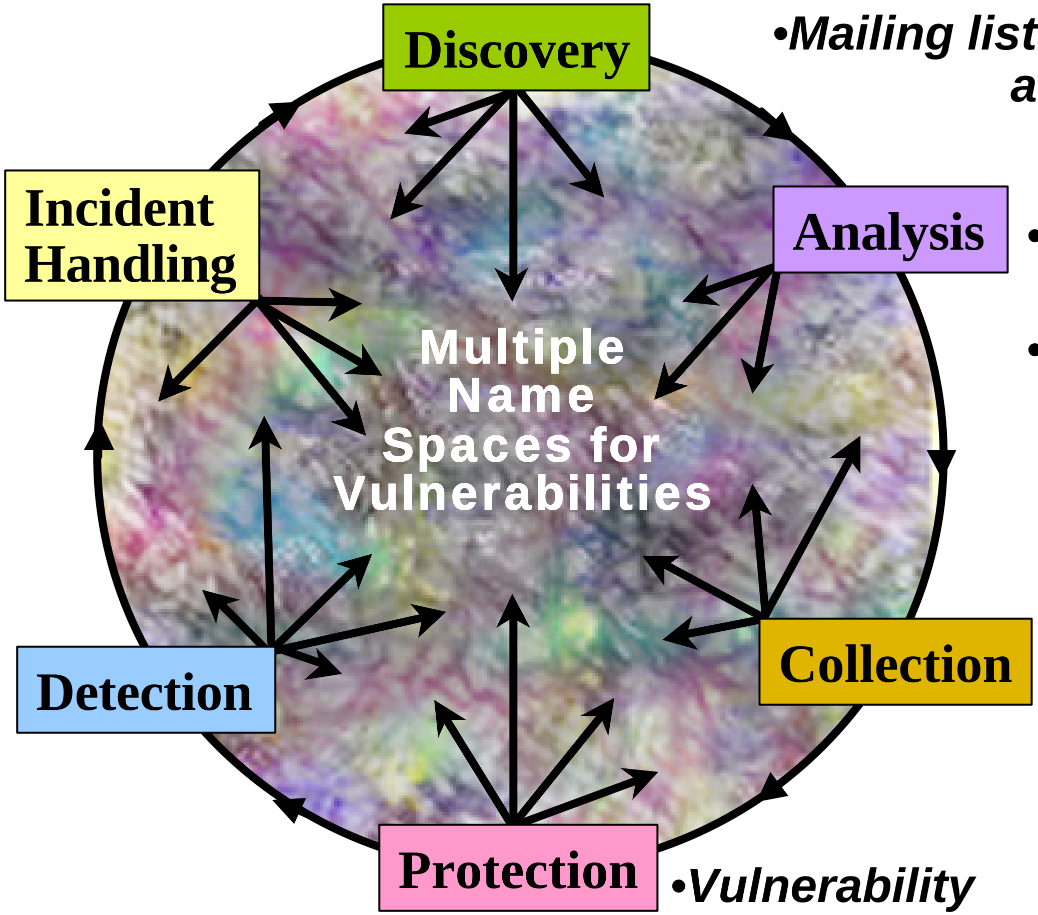
0 **Summary**

So how do you find out about commercial software vulnerabilities if the vendors aren’t going to tell you?

Three groups have emerged who share that same curiosity

- **Hackers**
  - want to find vulnerabilities and exposures so they can exploit them to gain access to systems
- **Commercial interests groups**
  - want to be hired to find, or want you to buy their tools to help you find, the vulnerabilities and exposures
  - offer services to come and do an evaluation of your systems
- **Philanthropists**
  - include security researchers in various government, academic, and non-profit organizations, as well as unaffiliated individuals that enjoy searching for vulnerabilities and exposures
  - usually share their knowledge and tools freely

There are Many Different types of Groups Involved in Providing Information about Vulnerabilities



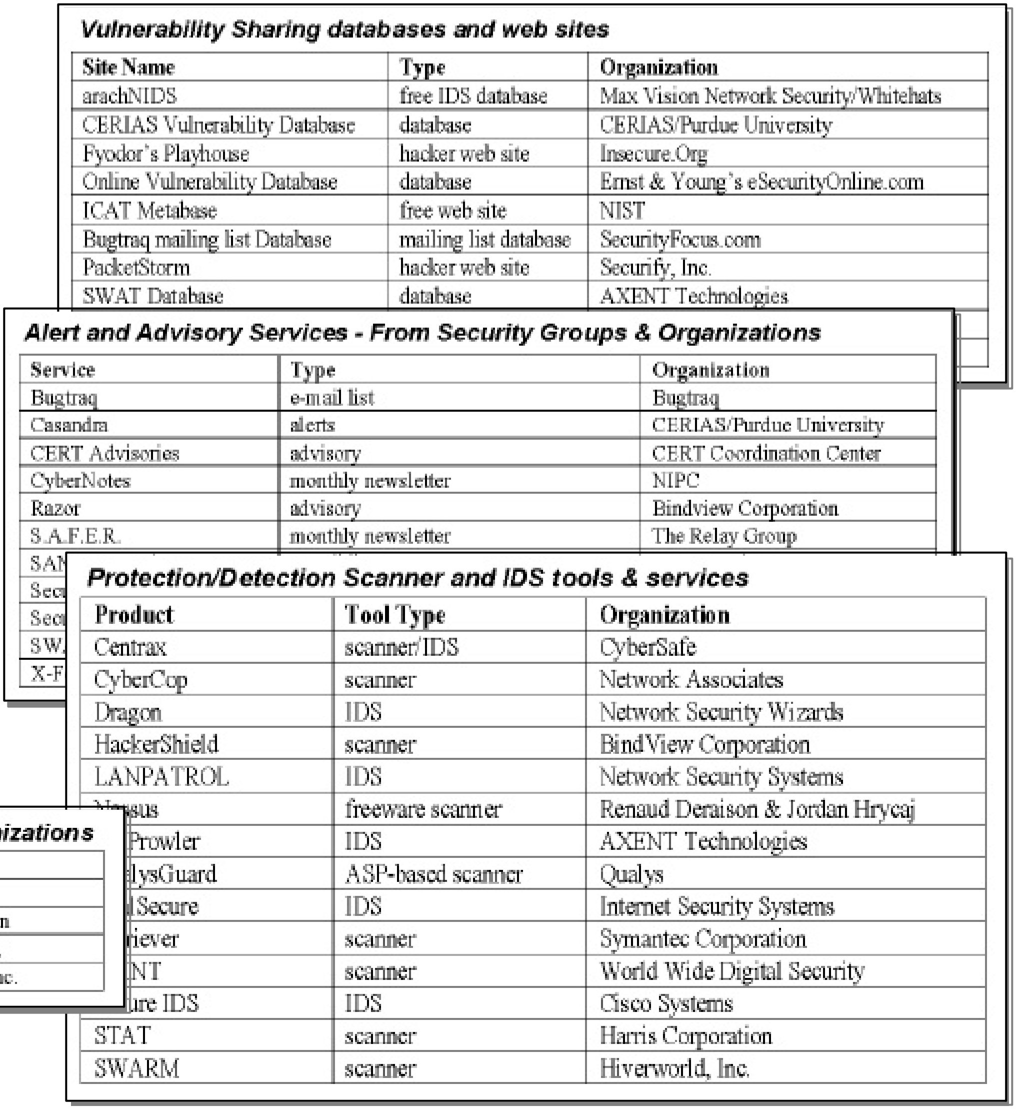
- *Mailing lists, Newsgroups, and Hacker sites*
- *Academic Studies*
- *Advisories*
- *Databases*
- *Newsletters*
- *Vulnerability Assessment Tools*
- *Intrusion Detection Systems*
- *Incident Response Teams*
- *Incident Reports*

The rule has been, "Whoever finds it, names it"

Implications of multiple name spaces for information on vulnerabilities

- Difficult to correlate data across multiple organizations and tools
  - IDS and assessment tools
  - Security tools and fix information
  - Incident information

- Difficult to conduct a detailed comparison of tools or databases (Vulnerabilities are counted differently)



Vulnerability Sharing databases and web sites

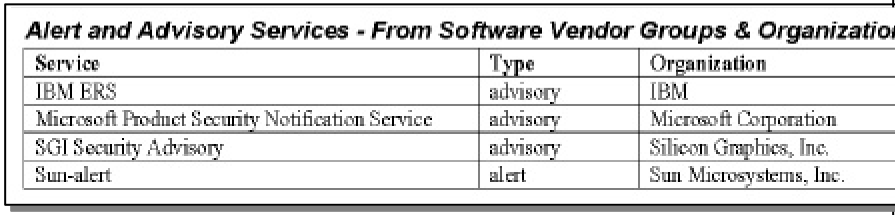
Site Name	Type	Organization
arachNIDS	free IDS database	Max Vision Network Security/Whitehats
CERIAS Vulnerability Database	database	CERIAS/Purdue University
Fyodor's Playhouse	hacker web site	Insecure.Org
Online Vulnerability Database	database	Ernst & Young's eSecurityOnline.com
ICAT Metabase	free web site	NIST
Bugtraq mailing list Database	mailing list database	SecurityFocus.com
PacketStorm	hacker web site	Securify, Inc.
SWAT Database	database	AXENT Technologies

Alert and Advisory Services - From Security Groups & Organizations

Service	Type	Organization
Bugtraq	e-mail list	Bugtraq
Casandra	alerts	CERIAS/Purdue University
CERT Advisories	advisory	CERT Coordination Center
CyberNotes	monthly newsletter	NIPC
Razor	advisory	Bindview Corporation
S.A.F.E.R.	monthly newsletter	The Relay Group
SAN		
Sec		
Sec		
SW		
X-F		

Protection/Detection Scanner and IDS tools & services

Product	Tool Type	Organization
Centrax	scanner/IDS	CyberSafe
CyberCop	scanner	Network Associates
Dragon	IDS	Network Security Wizards
HackerShield	scanner	BindView Corporation
LANPATROL	IDS	Network Security Systems
Nessus	freeware scanner	Renaud Deraison & Jordan Hrycaj
Prowler	IDS	AXENT Technologies
lysGuard	ASP-based scanner	Qualys
lSecure	IDS	Internet Security Systems
iever	scanner	Symantec Corporation
NT	scanner	World Wide Digital Security
ure IDS	IDS	Cisco Systems
STAT	scanner	Harris Corporation
SWARM	scanner	Hiverworld, Inc.



Alert and Advisory Services - From Software Vendor Groups & Organizations

Service	Type	Organization
IBM ERS	advisory	IBM
Microsoft Product Security Notification Service	advisory	Microsoft Corporation
SGI Security Advisory	advisory	Silicon Graphics, Inc.
Sun-alert	alert	Sun Microsystems, Inc.

Outline

0 **Background and Motivation**

0 **Finding Out About Vulnerabilities**

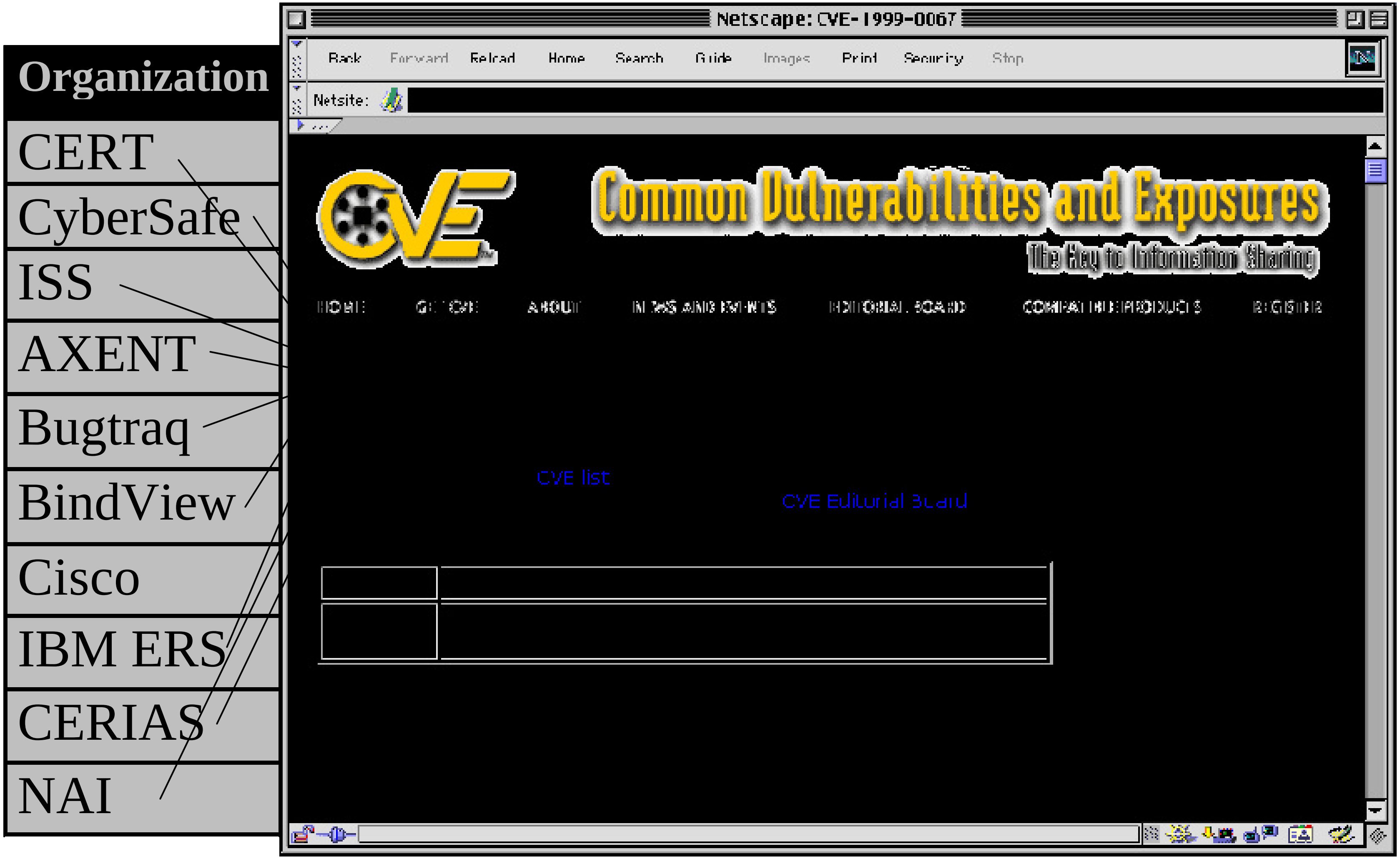
➡ **The Problem and a Solution - CVE**

0 **CVE Compatibility**

0 **The CVE Process**

0 **Summary**

The adoption of CVE Names by the Security Community is starting to address this problem

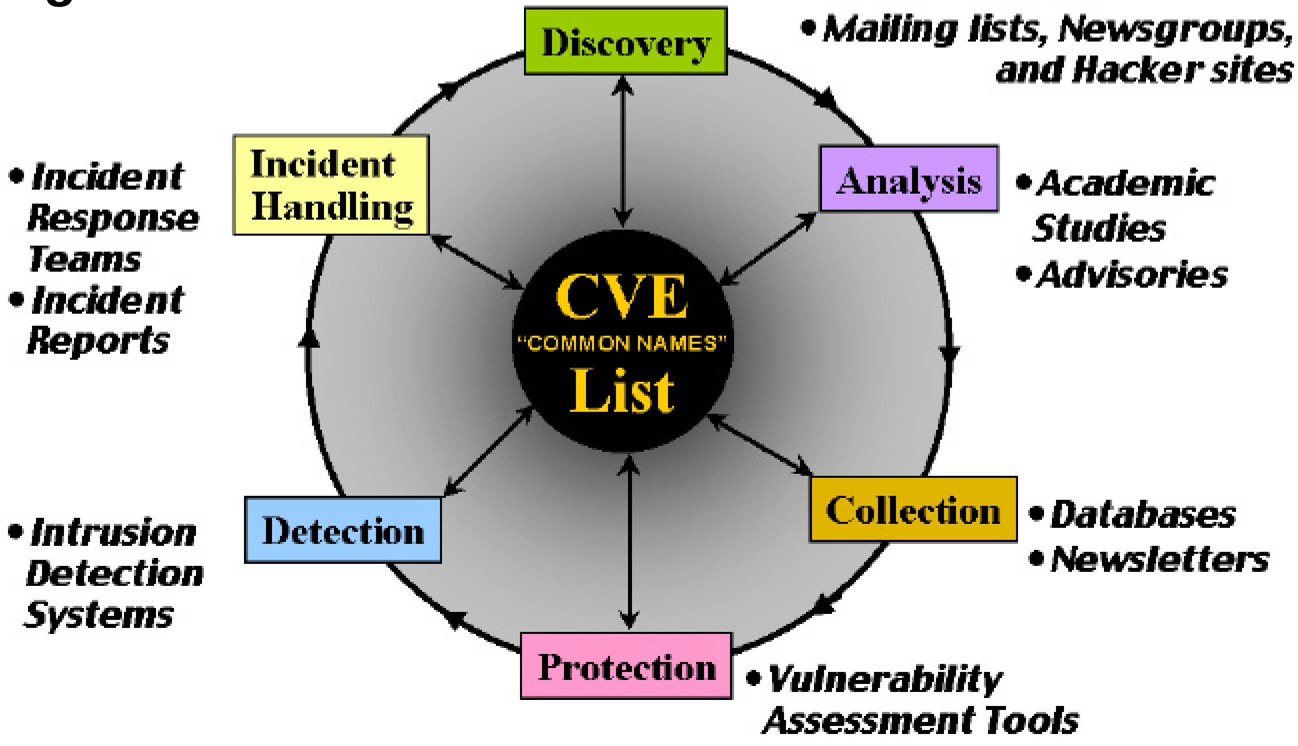


Organization
CERT
CyberSafe
ISS
AXENT
Bugtraq
BindView
Cisco
IBM ERS
CERIAS
NAI

Along with the new rule, "Whoever finds it, gets a CVE name for it"

The Vulnerability Information Sharing Process with CVE - - *"Whoever finds it, gets a CVE name for it"*

- Assigning a unique identifier to each problem
- Remaining independent of any particular perspective
  - Not just a developer's, researcher's, tester's, or analyst's view
- A community-wide effort via:
  - the CVE Editorial Board, the CVE Advisory Council, and the organizations adding CVE names into their tools, databases, web sites, & services
- Publicly open and shared
  - Will eventually list all publicly known security problems

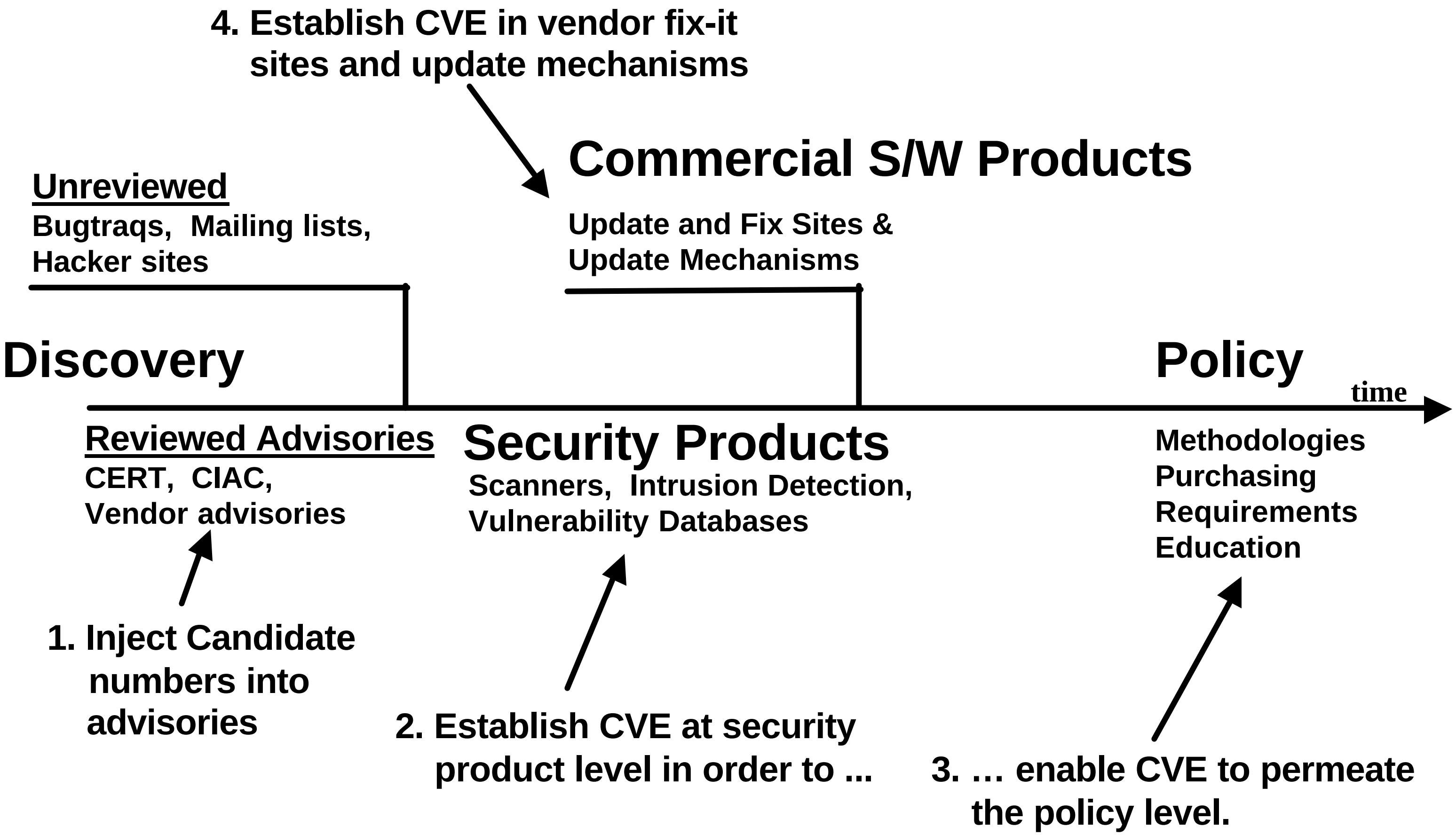


The Common Vulnerabilities and Exposures (CVE) Initiative

- An international security community activity led by MITRE focused on developing a list that provides common names for publicly known information security vulnerabilities and exposures.
- Key tenets
  - One name for one vulnerability or exposure
  - One standardized description for each vulnerability or exposure
  - Existence as a dictionary rather than a database
  - Publicly accessible for review or download from the Internet
  - Industry participation in open forum (editorial board)
- The CVE list and information about the CVE effort are available on the CVE web site at [cve.mitre.org]

1604 approved entries, 1880 being voted on, ~5000 under analysis, ~100-130 new/month

The CVE Strategy



4. Establish CVE in vendor fix-it sites and update mechanisms

Unreviewed

Bugtraqs, Mailing lists, Hacker sites

Commercial S/W Products

Update and Fix Sites & Update Mechanisms

Discovery

Policy

time

Reviewed Advisories

CERT, CIAC, Vendor advisories

Security Products

Scanners, Intrusion Detection, Vulnerability Databases

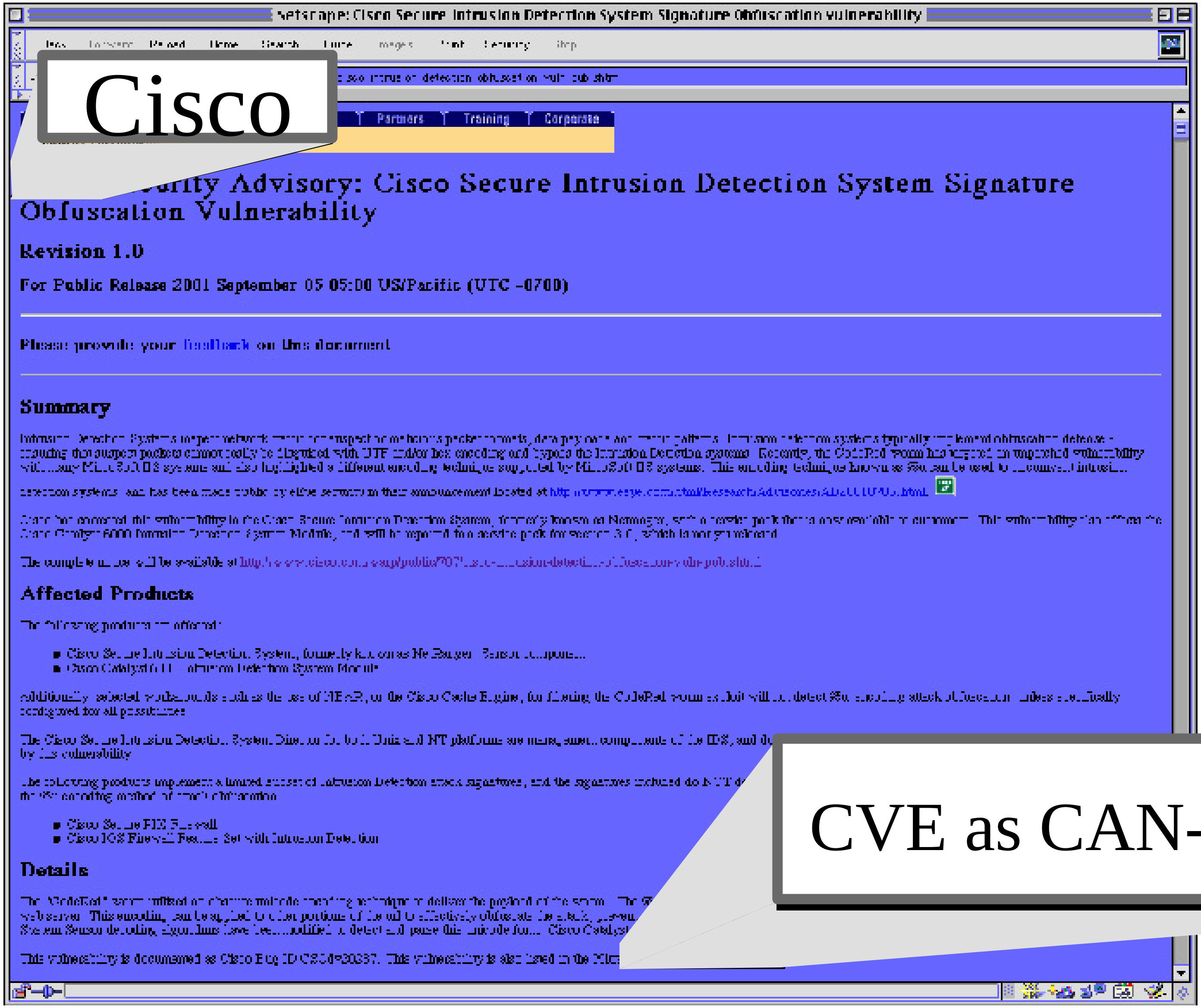
Methodologies
Purchasing
Requirements
Education

1. Inject Candidate numbers into advisories

2. Establish CVE at security product level in order to ...

3. … enable CVE to permeate the policy level.

The latest organization to start using CVE names in their alerts and advisories


Netscape: Cisco Secure Intrusion Detection System Signature Obfuscation Vulnerability
Partners
Training
Corporate

Cisco

…urity Advisory: Cisco Secure Intrusion Detection System Signature Obfuscation Vulnerability

Revision 1.0

For Public Release 2001 September 05 05:00 US/Pacific (UTC -0700)

Please provide your feedback on this document.

Summary

Intrusion Detection Systems inspect network traffic for suspect or malicious packet formats, data payloads and traffic patterns. Intrusion detection systems typically implement obfuscation defenses ensuring that suspect packets cannot easily be disguised with UTF and/or hex encoding and bypass the Intrusion Detection system. Recently, the CodeRed worm has exposed an unpatched vulnerability with many Microsoft IIS systems and also highlighted a different encoding technique supported by Microsoft IIS systems. This encoding technique known as %u can be used to circumvent intrusion detection systems, and has been made public by eEye security in their announcement located at http://www.eeye.com/html/Research/Advisories/AD20010705.html.

Cisco has corrected this vulnerability in the Cisco Secure Intrusion Detection System, formerly known as NetRanger, with a service pack that is now available to customers. This vulnerability also affects the Cisco Catalyst 6000 Intrusion Detection System Module, and will be repaired in a service pack for version 3.0, which is not yet released.

The complete notice will be available at http://www.cisco.com/warp/public/707/cisco-intrusion-detection-obfuscation-vuln-pub.shtml

Affected Products

The following products are affected:

- Cisco Secure Intrusion Detection System, formerly known as NetRanger, Sensor component
- Cisco Catalyst 6000 Intrusion Detection System Module

Additionally, selected workarounds such as the use of NBAR, or the Cisco Cache Engine, for filtering the CodeRed worm exploit will not detect %u encoding attack obfuscation unless specifically configured for all possibilities.

The Cisco Secure Intrusion Detection System Director for both Unix and NT platforms are management components of the IDS, and do … by this vulnerability.

The following products implement a limited subset of Intrusion Detection attack signatures, and the signatures included do NOT de… the %u encoding method of attack obfuscation.

- Cisco Secure PIX Firewall
- Cisco IOS Firewall Feature Set with Intrusion Detection

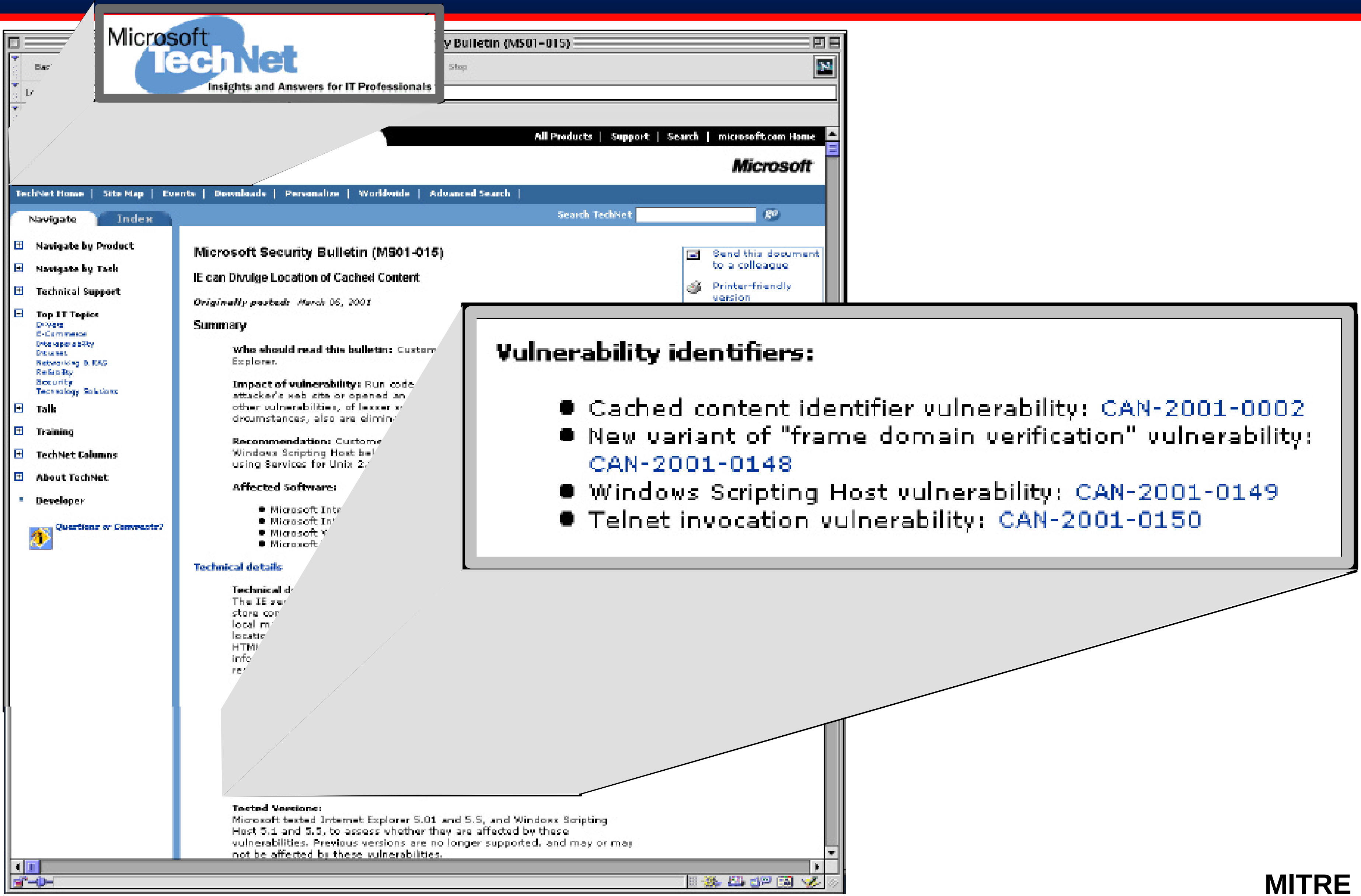
Details

The "CodeRed" worm utilized an alternate unicode encoding technique to deliver the payload of the worm. The %… web server. This encoding can be applied to other portions of the url to effectively obfuscate the attack, prevent… System Sensor decoding algorithms have been modified to detect and parse this unicode form. Cisco Catalyst…

This vulnerability is documented as Cisco Bug ID CSCdv20337. This vulnerability is also listed in the Mitre…

CVE as CAN-2001-0669.

The company with the most alerts using CVE names



Microsoft Security Bulletin (MS01-015)

IE can Divulge Location of Cached Content

Originally posted: March 06, 2001

Summary

Who should read this bulletin: Custom
Explorer.

Impact of vulnerability: Run code
attacker's web site or opened an
other vulnerabilities, of lesser s
circumstances, also are elimin

Recommendation: Custome
Windows Scripting Host bel
using Services for Unix 2.

Affected Software:

- Microsoft Inte
- Microsoft Int
- Microsoft Y
- Microsoft

Technical details

Technical d
The IE ser
store cor
local m
locatic
HTML
info
re

Tested Versions:
Microsoft tested Internet Explorer 5.01 and 5.5, and Windows Scripting Host 5.1 and 5.5, to assess whether they are affected by these vulnerabilities. Previous versions are no longer supported, and may or may not be affected by these vulnerabilities.

Vulnerability identifiers:

- Cached content identifier vulnerability: CAN-2001-0002
- New variant of "frame domain verification" vulnerability: CAN-2001-0148
- Windows Scripting Host vulnerability: CAN-2001-0149
- Telnet invocation vulnerability: CAN-2001-0150

Outline

0 **Background and Motivation**
0 **Finding Out About Vulnerabilities**
0 **The Problem and a Solution - CVE**
➡ **CVE Compatibility**
0 **The CVE Process**
0 **Summary**

What does CVE-compatible mean?

- CVE-compatible means that a tool or database can “speak CVE” and correlate data with other CVE-compatible products

- CVE-compatible means it meets the following requirements:
  - Can find items by CVE name (CVE searchable)
  - Includes CVE name in output for each item (CVE output)
  - Provided MITRE with “vulnerability” item mappings to validate the accuracy of the product or services CVE entries
  - Makes a good faith effort to keep mappings accurate

Organizations With Products That Use CVE

(as of 15 October 2001)

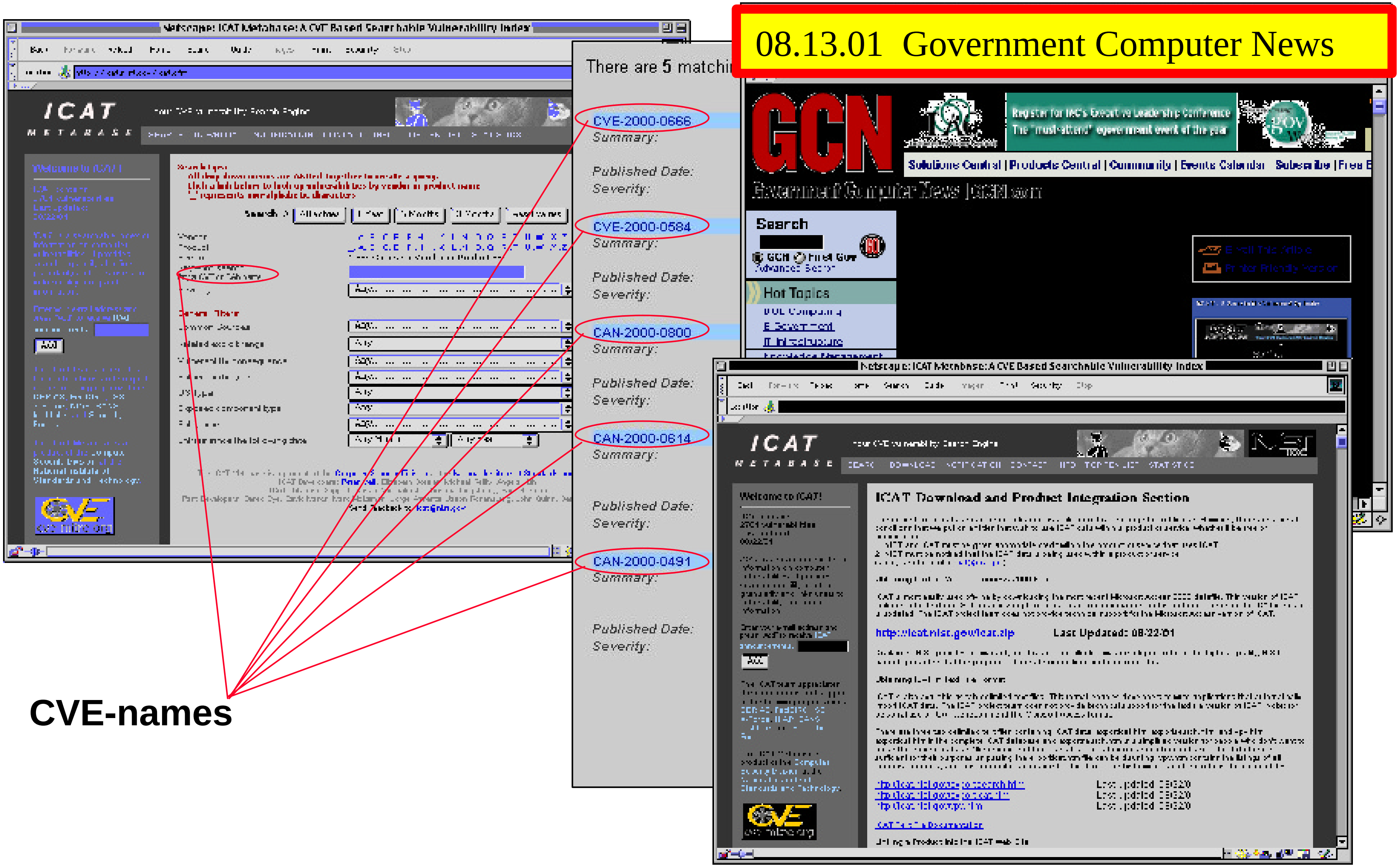
0 **These organizations have publicly declared that they are working on (over 60) CVE-compatible tools, databases, web sites, or services**

Advanced Research Corp
Alliance Qualité Logiciel
BindView Development
CERIAS/Purdue University
CERT Coordination Center
Cisco Systems
CS&S Corportation
CyberSafe
CYRANO
UC Davis
Enterasys Networks ***(bought Network Security Wizards)***
Entercept Security Technologies
Ernst & Young
Foundstone, Inc.
Harris Corporation
Intranode
Intrusion.com
Internet Security Systems
LURHQ Corporation
Max Vision Network Security/Whitehats

nCircle ***(formerly Hiverworld)***
The Nessus Project
Network Security Systems
NIST
nSecure Software (P) LTD.
NTBugtraq
Penta Security Systems
PGP Security, NAI
Qualys
SANS
Security Focus, Inc.
SecurityWatch
spiDYNAMICS
Symantec
Tiger Testing
Tivoli Systems Inc.
Tsinghua UnisNet Technology, Ltd.
Venus Information Technology Inc.
World Wide Digital Security

Up-to-date list at http://cve.mitre.org/compatible

Examples of CVE-compatible items:
The ICAT Metabase



08.13.01 Government Computer News

There are 5 matchi

CVE-2000-0666
Summary:
Published Date:
Severity:

CVE-2000-0584
Summary:
Published Date:
Severity:

CAN-2000-0800
Summary:
Published Date:
Severity:

CAN-2000-0614
Summary:
Published Date:
Severity:

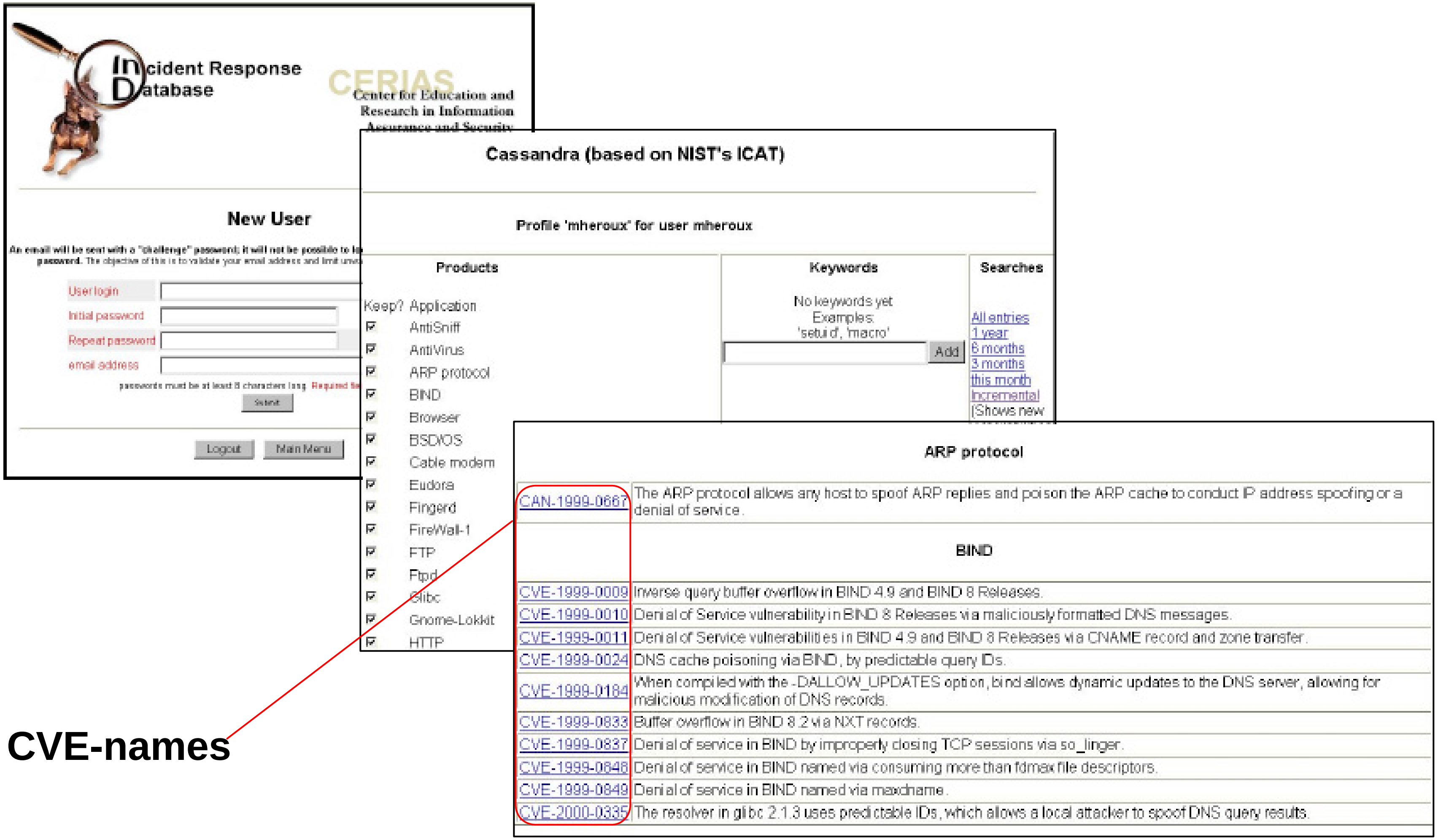
CAN-2000-0491
Summary:
Published Date:
Severity:

Netscape: ICAT Metabase: A CVE Based Searchable Vulnerability Index
ICAT METABASE
GCN
Government Computer News | GCN.com
Search
Hot Topics
ICAT Download and Product Integration Section
http://icat.nist.gov/icat.zip
Last Updated: 08-22-01
cve.mitre.org

CVE-names

http://icat.nist.gov

Examples continued: *Cassandra*



Incident Response Database
CERIAS
Center for Education and Research in Information Assurance and Security

New User

An email will be sent with a "challenge" password; it will not be possible to lo
password. The objective of this is to validate your email address and limit unva

User login
Initial password
Repeat password
email address

passwords must be at least 8 characters long. Required fie

Cassandra (based on NIST's ICAT)

Profile 'mheroux' for user mheroux

Products

Keep?	Application
☑	AntiSniff
☑	AntiVirus
☑	ARP protocol
☑	BIND
☑	Browser
☑	BSD/OS
☑	Cable modem
☑	Eudora
☑	Fingerd
☑	FireWall-1
☑	FTP
☑	Ftpd
☑	Glibc
☑	Gnome-Lokkit
☑	HTTP

Keywords

No keywords yet
Examples:
'setuid', 'macro'

Searches

All entries
1 year
6 months
3 months
this month
Incremental
(Shows new

ARP protocol

CAN-1999-0667	The ARP protocol allows any host to spoof ARP replies and poison the ARP cache to conduct IP address spoofing or a denial of service.

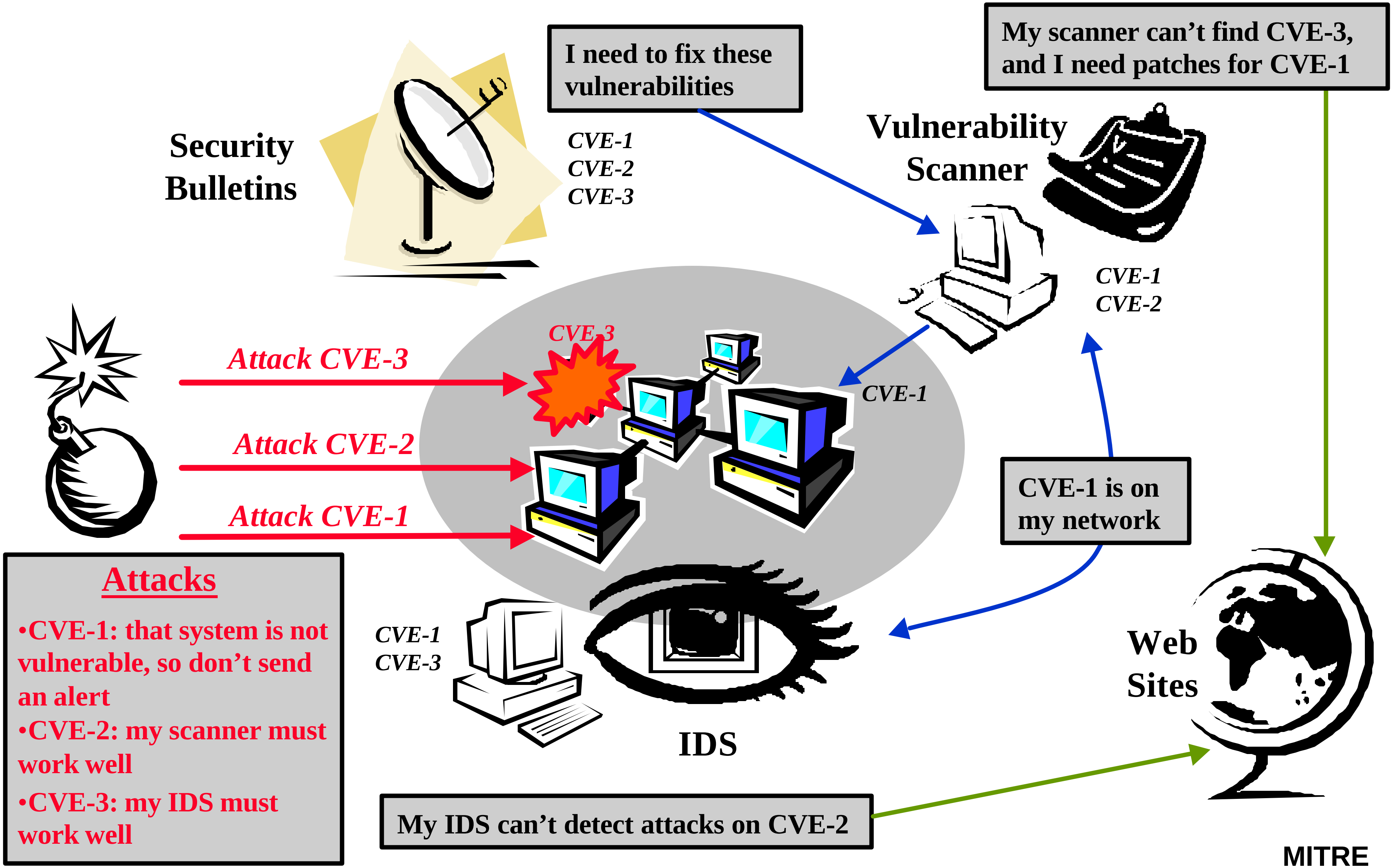
BIND

CVE-1999-0009	Inverse query buffer overflow in BIND 4.9 and BIND 8 Releases.
CVE-1999-0010	Denial of Service vulnerability in BIND 8 Releases via maliciously formatted DNS messages.
CVE-1999-0011	Denial of Service vulnerabilities in BIND 4.9 and BIND 8 Releases via CNAME record and zone transfer.
CVE-1999-0024	DNS cache poisoning via BIND, by predictable query IDs.
CVE-1999-0184	When compiled with the -DALLOW_UPDATES option, bind allows dynamic updates to the DNS server, allowing for malicious modification of DNS records.
CVE-1999-0833	Buffer overflow in BIND 8.2 via NXT records.
CVE-1999-0837	Denial of service in BIND by improperly closing TCP sessions via so_linger.
CVE-1999-0848	Denial of service in BIND named via consuming more than fdmax file descriptors.
CVE-1999-0849	Denial of service in BIND named via maxdname.
CVE-2000-0335	The resolver in glibc 2.1.3 uses predictable IDs, which allows a local attacker to spoof DNS query results.

CVE-names

https://cassandra.cerias.purdue.edu

Using CVE in the Enterprise



Security Bulletins

CVE-1
CVE-2
CVE-3

I need to fix these vulnerabilities

My scanner can't find CVE-3, and I need patches for CVE-1

Vulnerability Scanner

CVE-1
CVE-2

CVE-3

Attack CVE-3

Attack CVE-2

Attack CVE-1

CVE-1

CVE-1 is on my network

Web Sites

CVE-1
CVE-3

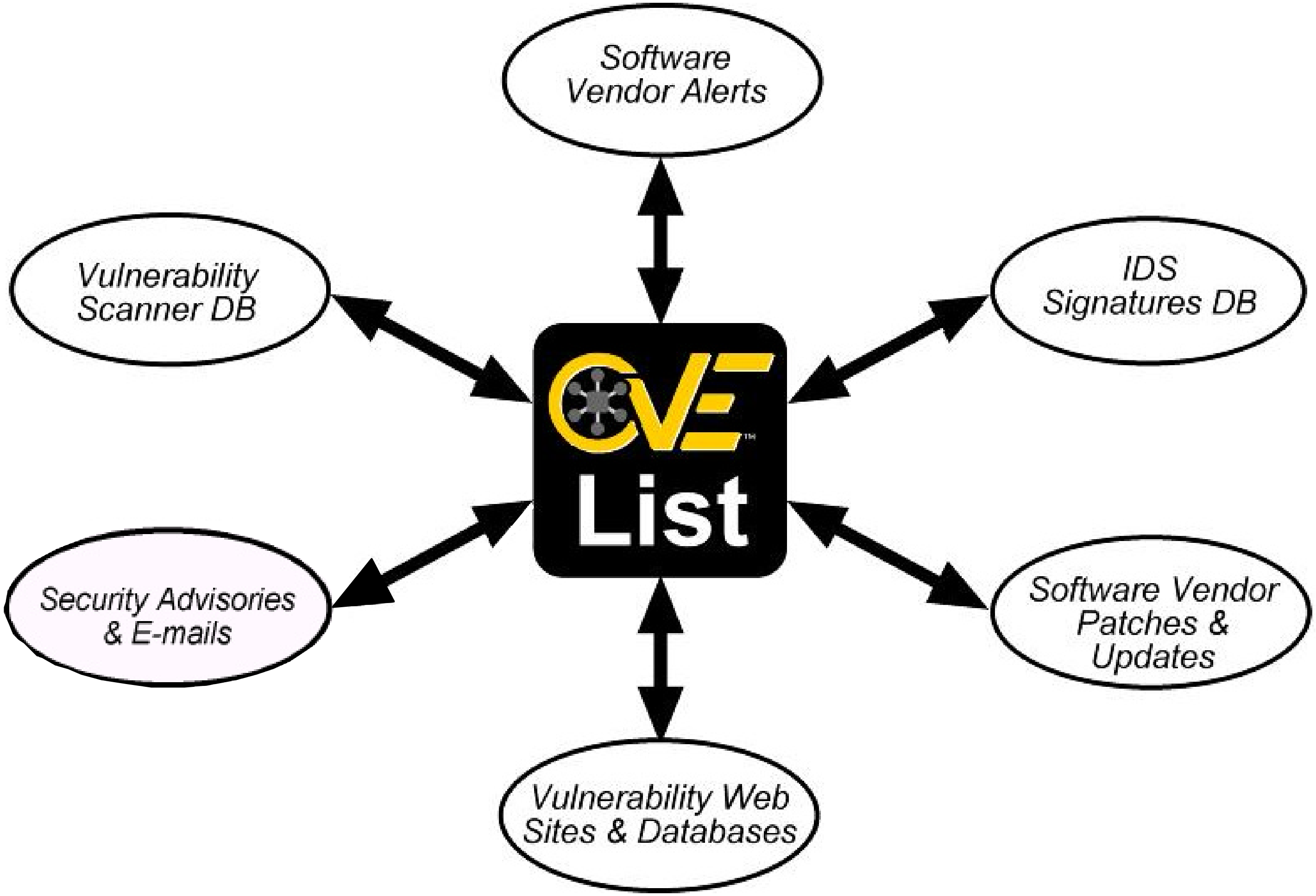
IDS

My IDS can't detect attacks on CVE-2

Attacks

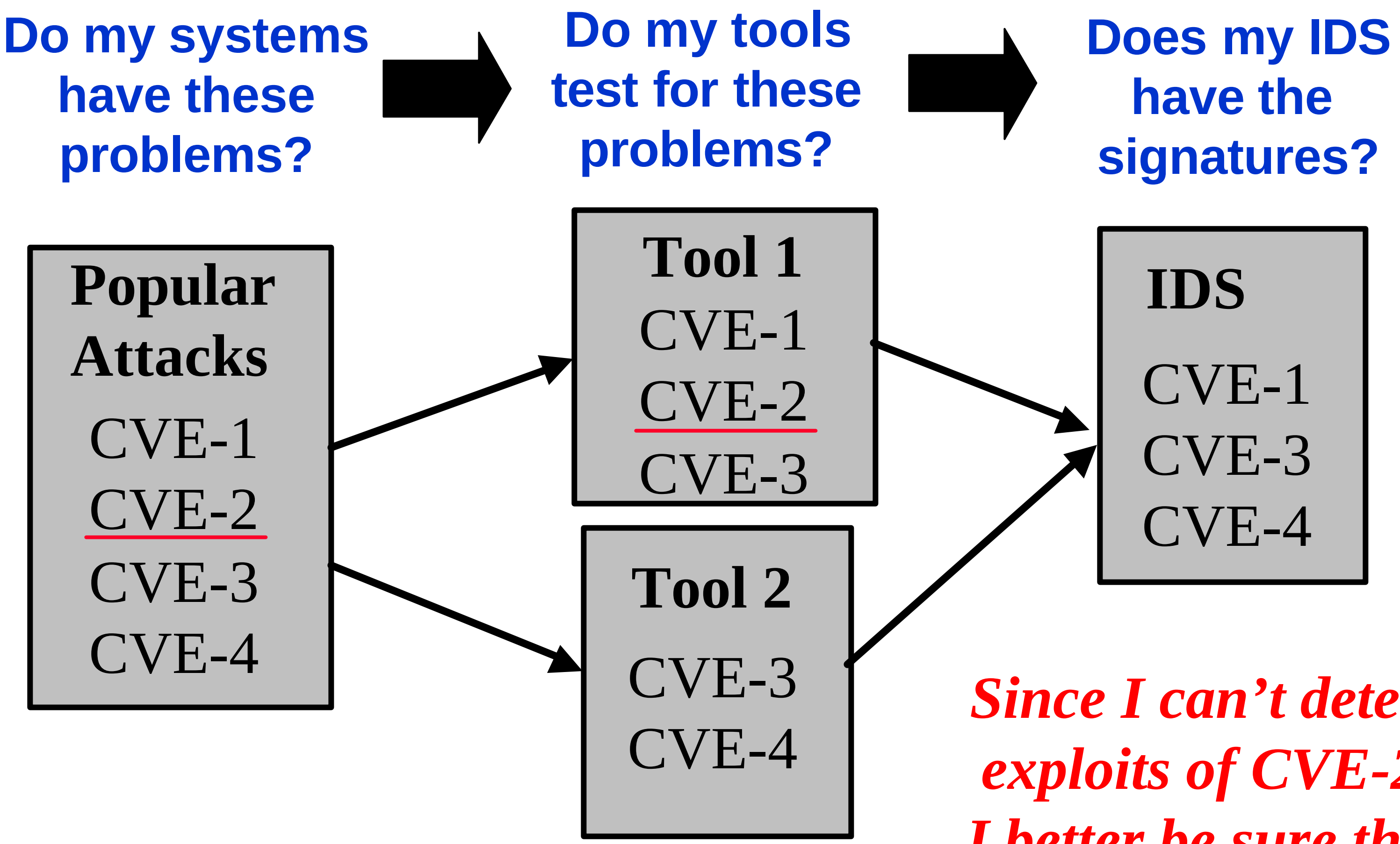
- •CVE-1: that system is not vulnerable, so don't send an alert
- •CVE-2: my scanner must work well
- •CVE-3: my IDS must work well

CVE compatibility provides a path for integrating information on Vulnerabilities and Exposures


Software Vendor Alerts
Vulnerability Scanner DB
IDS Signatures DB
CVE™
List
Security Advisories & E-mails
Software Vendor Patches & Updates
Vulnerability Web Sites & Databases

CVE compatibility means that a tool or database can "speak CVE" and correlate data with other CVE-compatible products.

Example using CVE compatibility to go from Advisories to Vulnerability Scanners to IDSes



Do my systems have these problems?

Do my tools test for these problems?

Does my IDS have the signatures?

Popular Attacks

CVE-1

CVE-2

CVE-3

CVE-4

Tool 1

CVE-1

CVE-2

CVE-3

Tool 2

CVE-3

CVE-4

IDS

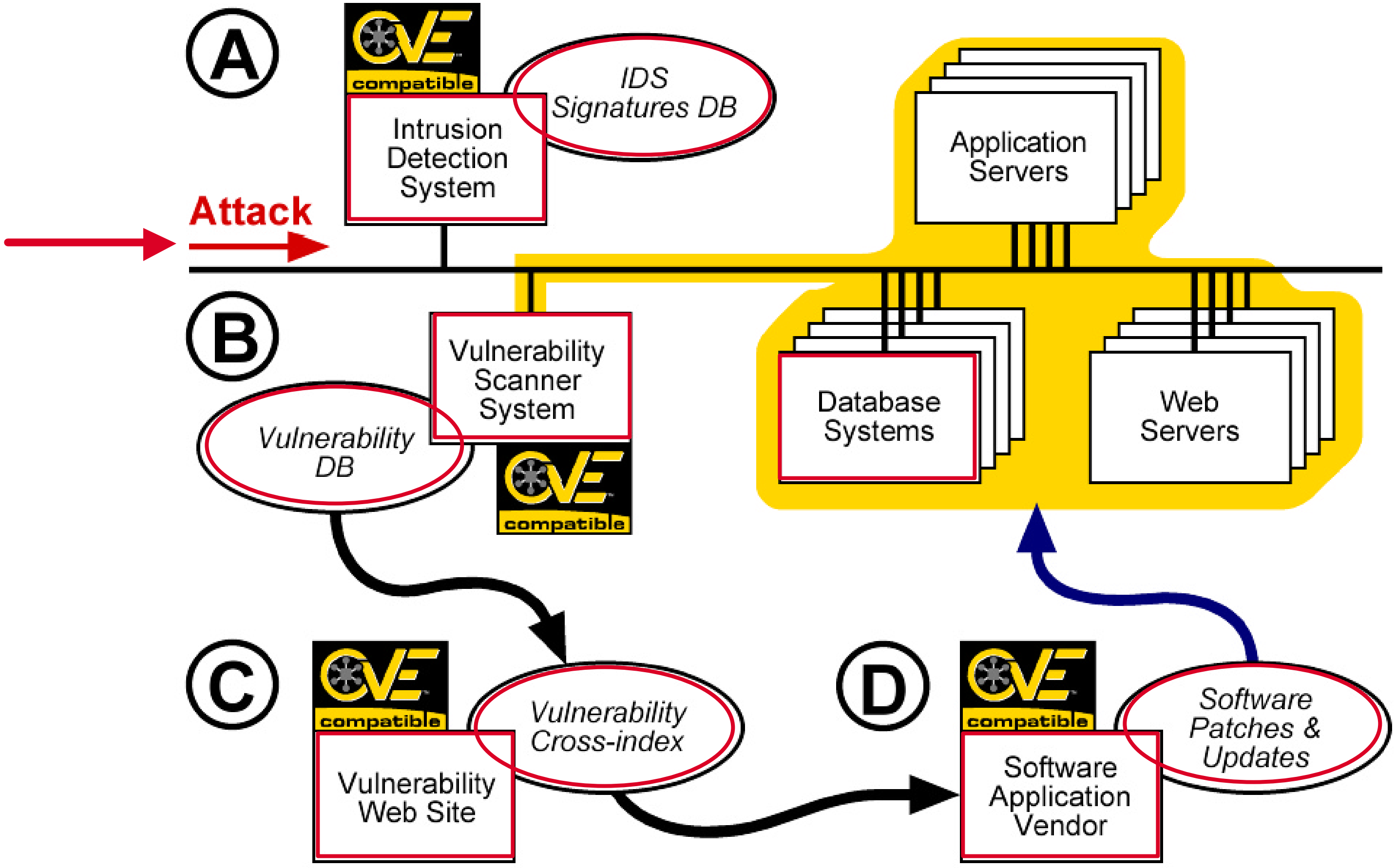
CVE-1

CVE-3

CVE-4

Since I can’t detect exploits of CVE-2 I better be sure that Tool 1 is real good at checking for it.

A CVE-Enabled Process Leverages CVE compatibility



Outline

0 **Background and Motivation**

0 **Finding Out About Vulnerabilities**

0 **The Problem and a Solution - CVE**

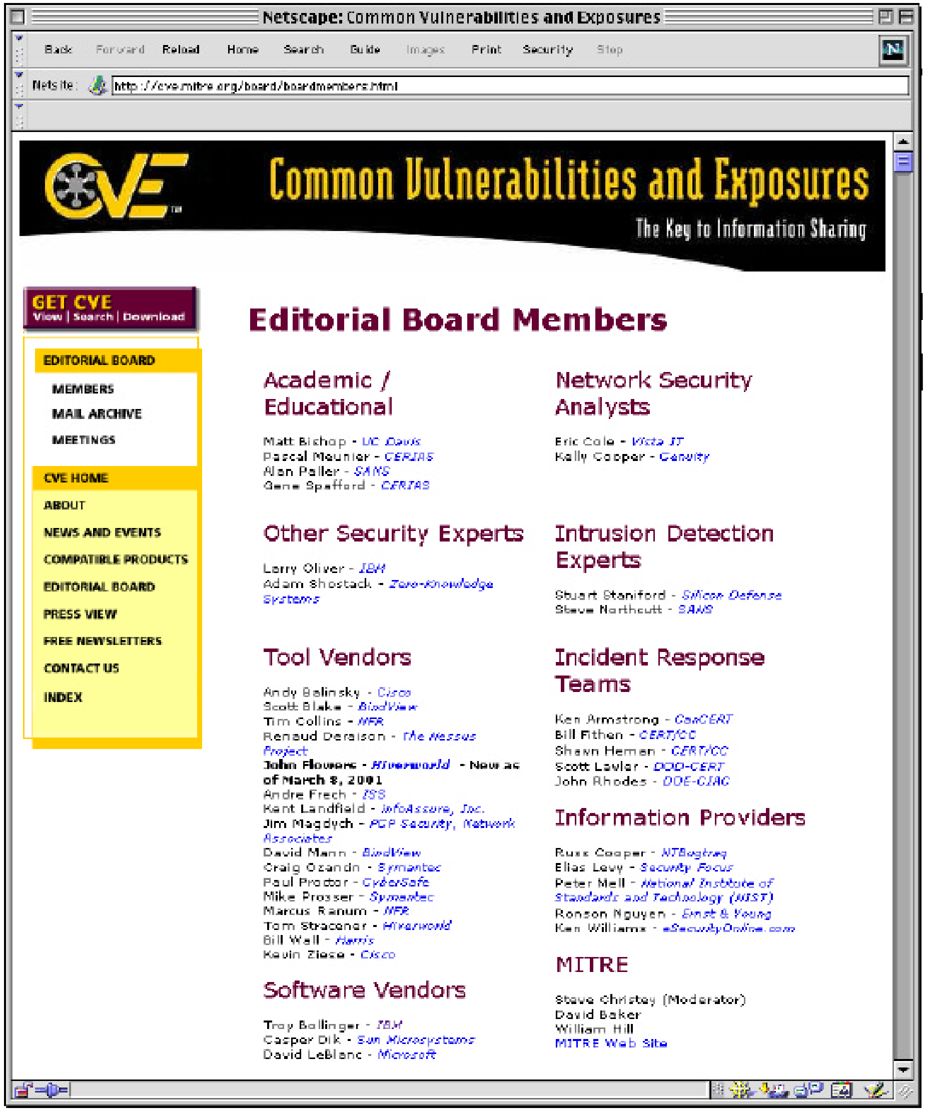
0 **CVE Compatibility**

➤ **The CVE Process**

0 **Summary**

CVE Editorial Board

- 0 **Includes mostly technical representatives from 30 different organizations including researchers, tool vendors, response teams, and end users**
- 0 **Reviews and approves CVE entries**
- 0 **Discusses issues related to CVE maintenance**
- 0 **Holds monthly meetings (face-to-face or phone)**
- 0 **Maintains publicly viewable mailing list archives**
  [cve.mitre.org/board/archives]



Editorial Board Members

Academic / Educational

Matt Bishop - *UC Davis*
Pascal Meunier - *CERIAS*
Alan Paller - *SANS*
Gene Spafford - *CERIAS*

Other Security Experts

Larry Oliver - *IBM*
Adam Shostack - *Zero-Knowledge Systems*

Tool Vendors

Andy Balinsky - *Cisco*
Scott Blake - *BindView*
Tim Collins - *NFR*
Renaud Deraison - *The Nessus Project*
John Flowers - *Hiverworld* - New as of March 8, 2001
Andre Frech - *ISS*
Kent Landfield - *InfoAssure, Inc.*
Jim Magdych - *PGP Security, Network Associates*
David Mann - *BindView*
Craig Ozancin - *Symantec*
Paul Proctor - *CyberSafe*
Mike Prosser - *Symantec*
Marcus Ranum - *NFR*
Tom Stracener - *Hiverworld*
Bill Wall - *Harris*
Kevin Ziese - *Cisco*

Software Vendors

Troy Bollinger - *IBM*
Casper Dik - *Sun Microsystems*
David LeBlanc - *Microsoft*

Network Security Analysts

Eric Cole - *Vista IT*
Kelly Cooper - *Genuity*

Intrusion Detection Experts

Stuart Staniford - *Silicon Defense*
Steve Northcutt - *SANS*

Incident Response Teams

Ken Armstrong - *CanCERT*
Bill Fithen - *CERT/CC*
Shawn Hernan - *CERT/CC*
Scott Lawler - *DOD-CERT*
John Rhodes - *DOE-CIAC*

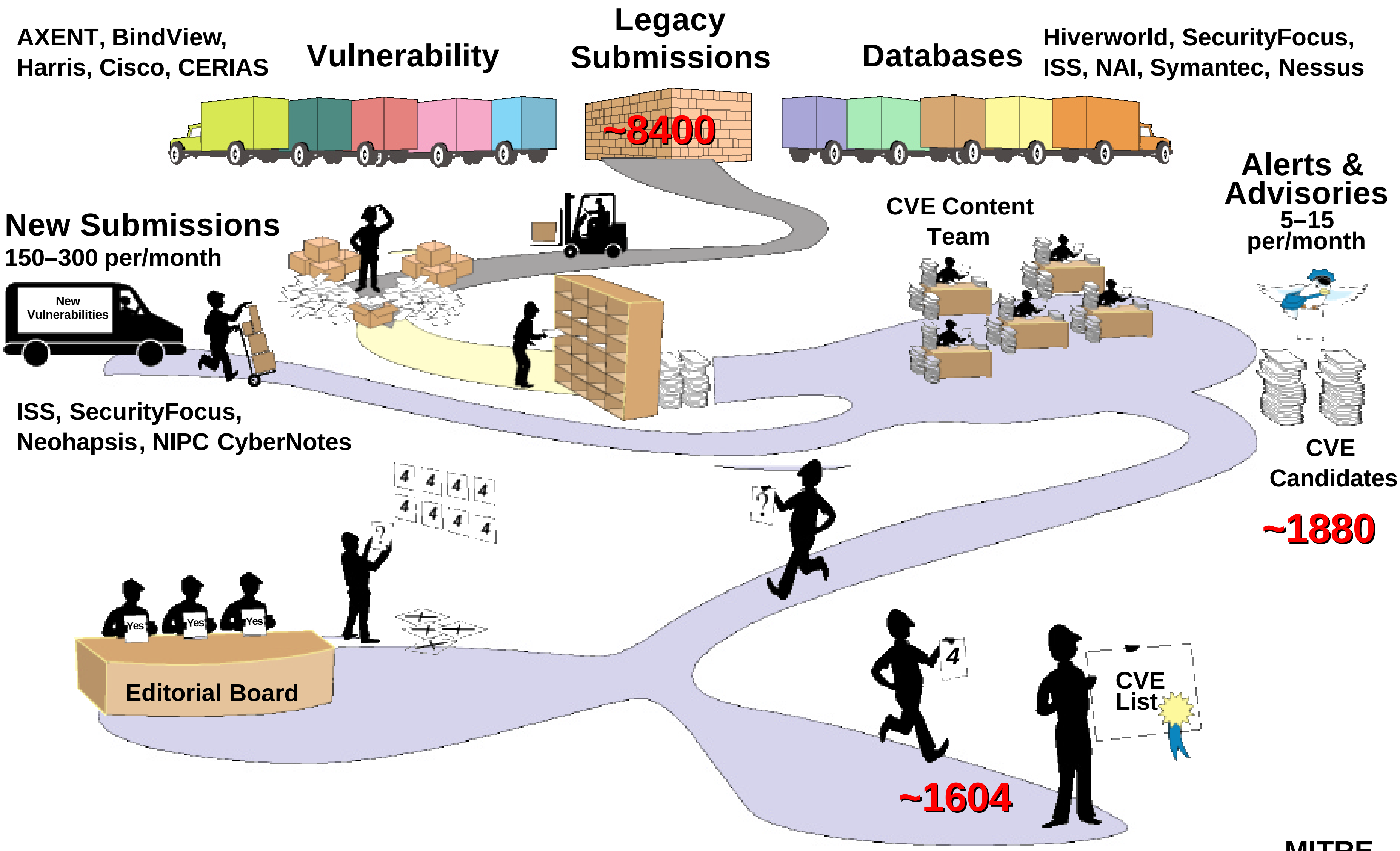
Information Providers

Russ Cooper - *NTBugtraq*
Elias Levy - *Security Focus*
Peter Mell - *National Institute of Standards and Technology (NIST)*
Ronson Nguyen - *Ernst & Young*
Ken Williams - *eSecurityOnline.com*

MITRE

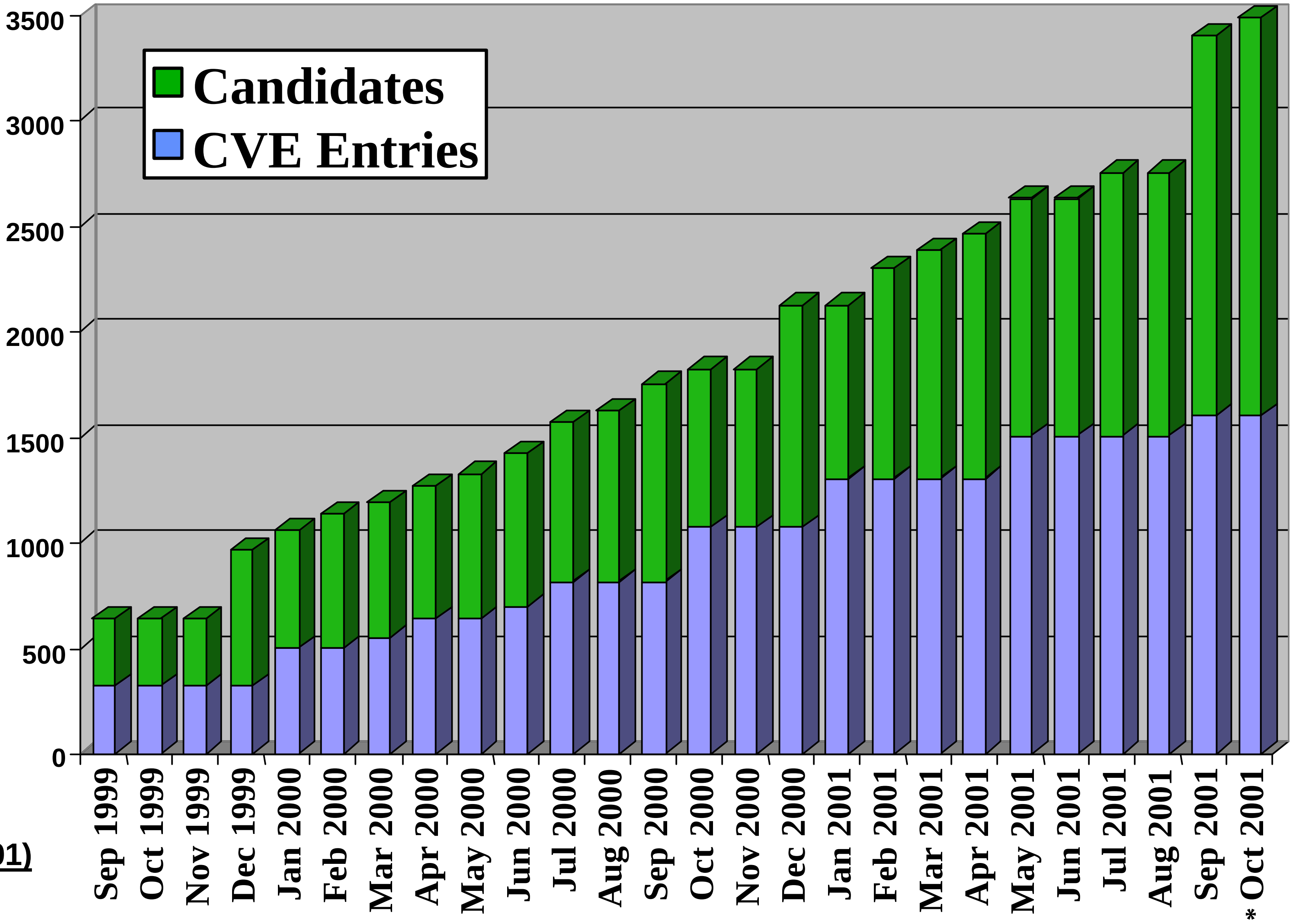
Steve Christey (Moderator)
David Baker
William Hill
MITRE Web Site

Where the CVE List comes from



MITRE

CVE Growth

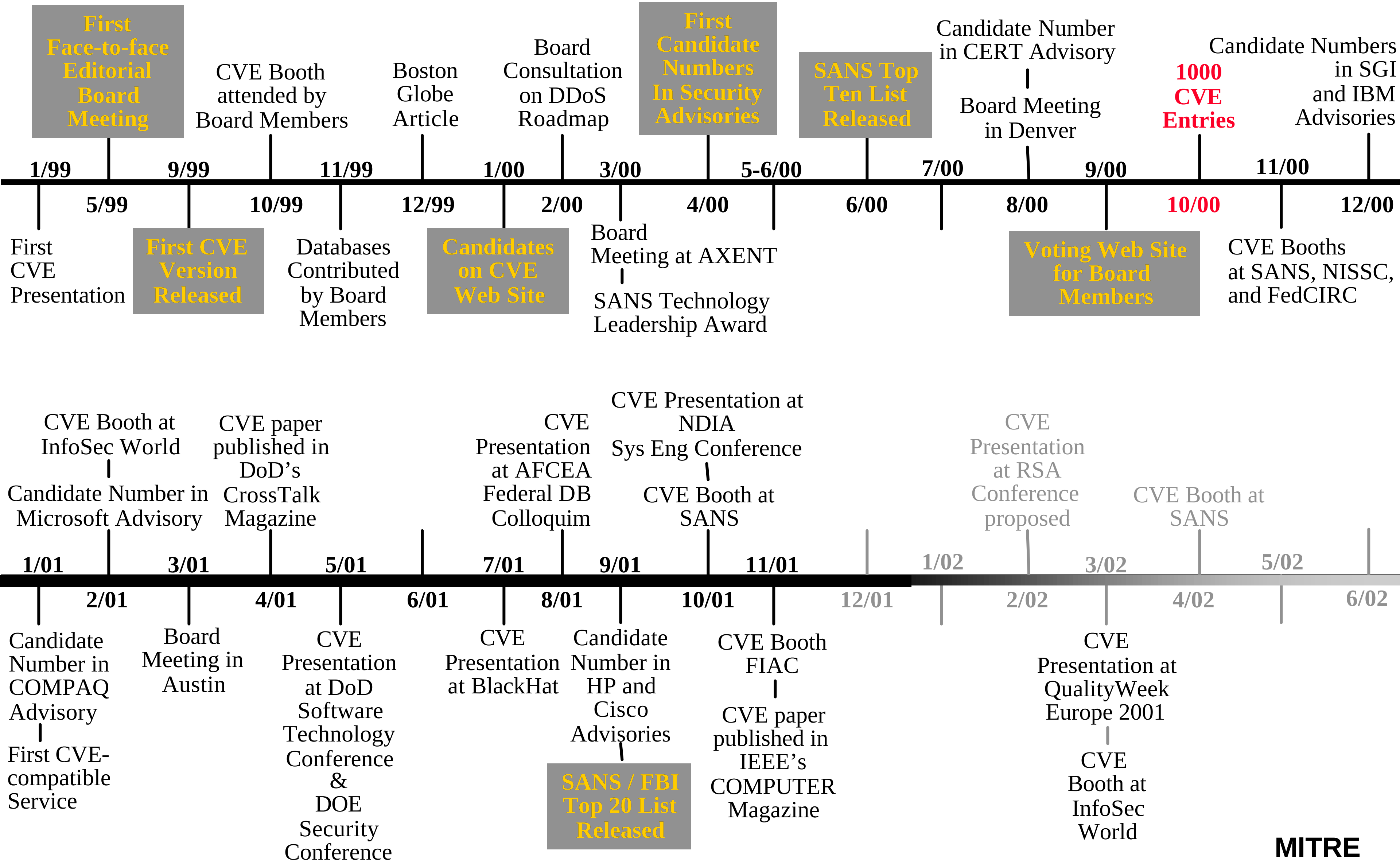


Status

(as of Oct 15, 2001)

- **1604 entries**
- **1880 candidates**

Major CVE Milestones



First Face-to-face Editorial Board Meeting

CVE Booth attended by Board Members

Boston Globe Article

Board Consultation on DDoS Roadmap

First Candidate Numbers In Security Advisories

SANS Top Ten List Released

Candidate Number in CERT Advisory | Board Meeting in Denver

1000 CVE Entries

Candidate Numbers in SGI and IBM Advisories

1/99 5/99 9/99 10/99 11/99 12/99 1/00 2/00 3/00 4/00 5-6/00 6/00 7/00 8/00 9/00 10/00 11/00 12/00

First CVE Presentation

First CVE Version Released

Databases Contributed by Board Members

Candidates on CVE Web Site

Board Meeting at AXENT | SANS Technology Leadership Award

Voting Web Site for Board Members

CVE Booths at SANS, NISSC, and FedCIRC

CVE Booth at InfoSec World | Candidate Number in Microsoft Advisory

CVE paper published in DoD's CrossTalk Magazine

CVE Presentation at AFCEA Federal DB Colloquim

CVE Presentation at NDIA Sys Eng Conference | CVE Booth at SANS

CVE Presentation at RSA Conference proposed

CVE Booth at SANS

1/01 2/01 3/01 4/01 5/01 6/01 7/01 8/01 9/01 10/01 11/01 12/01 1/02 2/02 3/02 4/02 5/02 6/02

Candidate Number in COMPAQ Advisory | First CVE-compatible Service

Board Meeting in Austin

CVE Presentation at DoD Software Technology Conference & DOE Security Conference

CVE Presentation at BlackHat

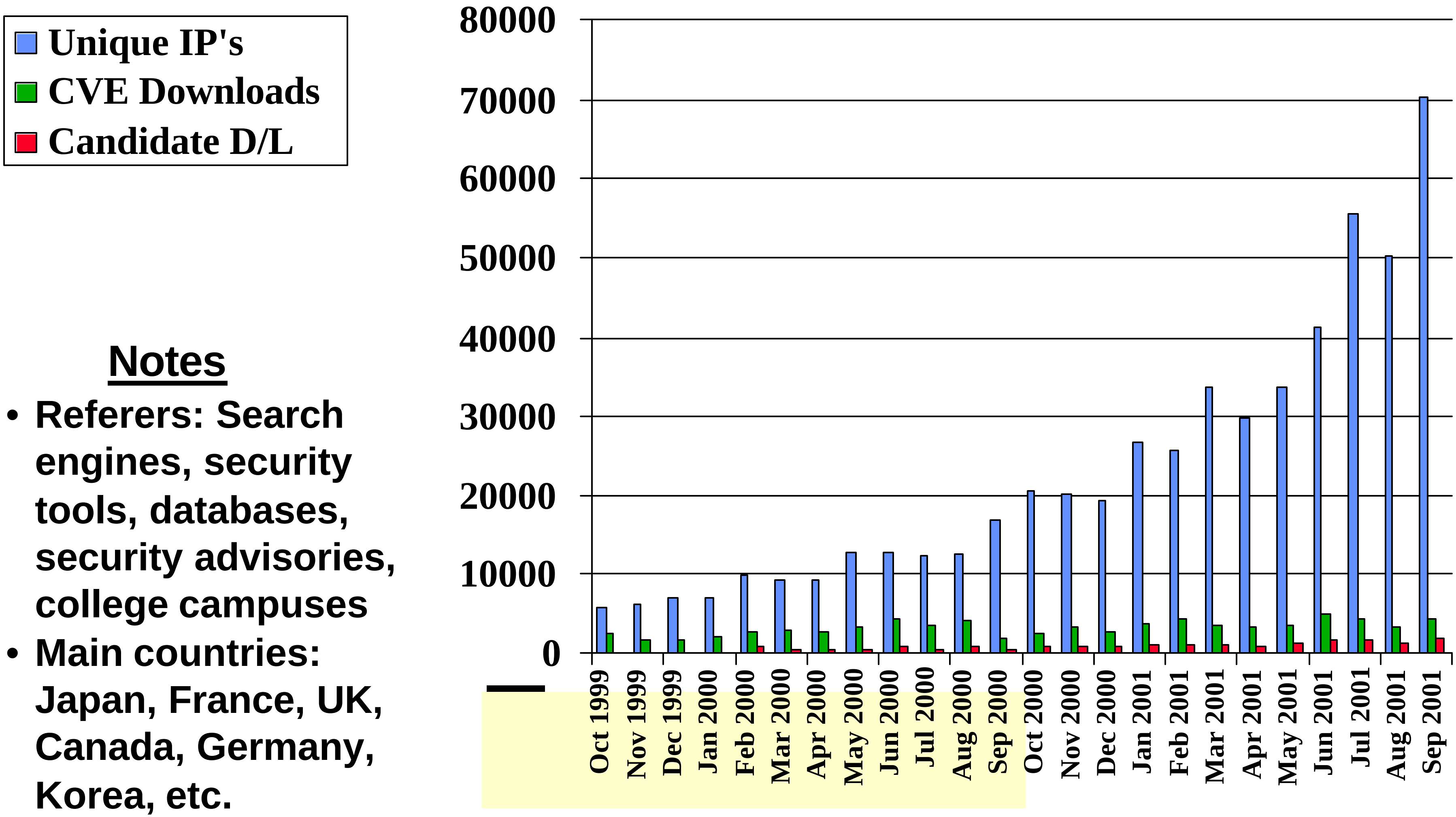
Candidate Number in HP and Cisco Advisories | **SANS / FBI Top 20 List Released**

CVE Booth FIAC | CVE paper published in IEEE's COMPUTER Magazine

CVE Presentation at QualityWeek Europe 2001 | CVE Booth at InfoSec World

MITRE

CVE Web Site Statistics



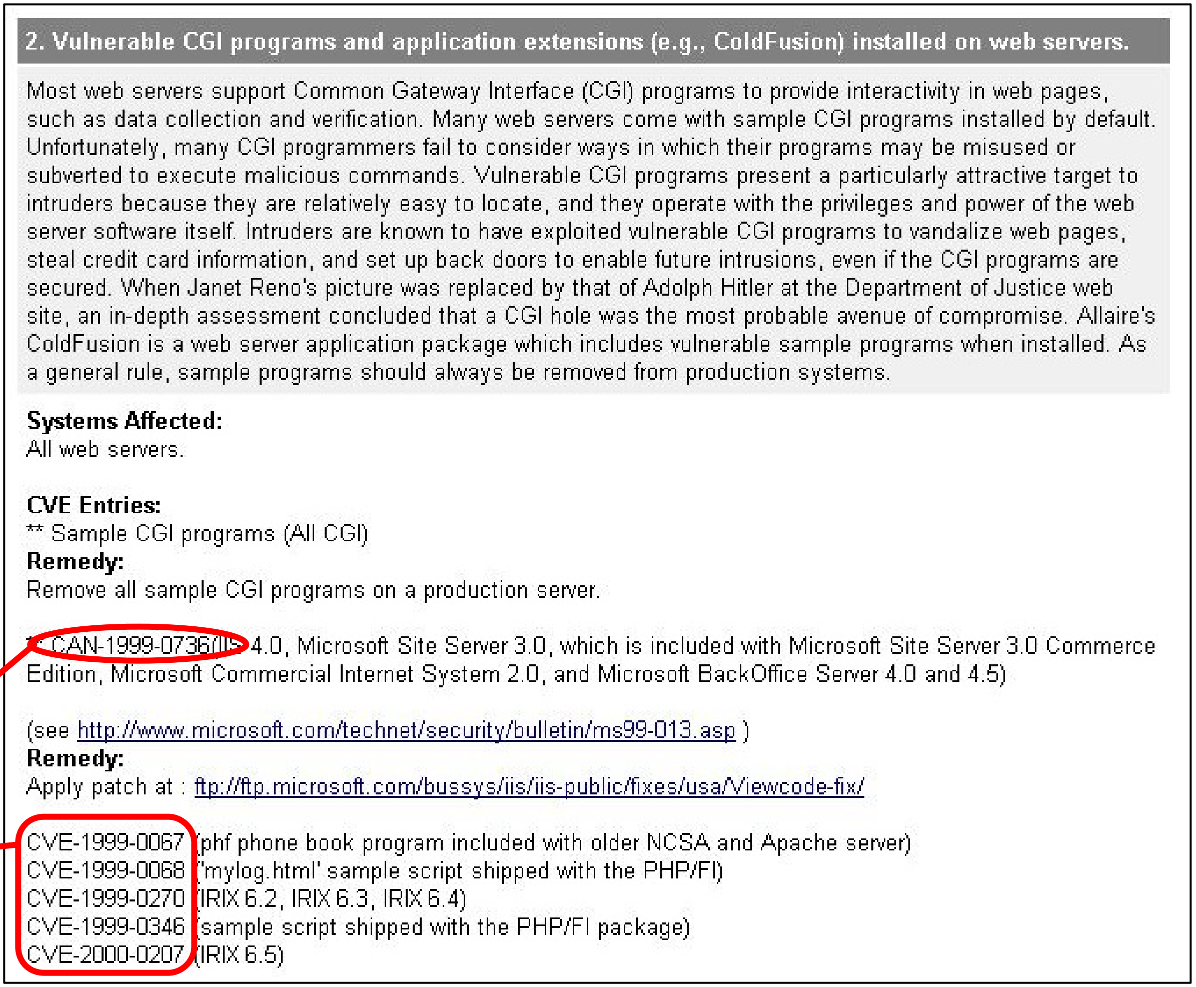
Notes

- Referers: Search engines, security tools, databases, security advisories, college campuses
- Main countries: Japan, France, UK, Canada, Germany, Korea, etc.

Outline

- 0 **Background and Motivation**
- 0 **Finding Out About Vulnerabilities**
- 0 **The Problem and a Solution - CVE**
- 0 **CVE Compatibility**
- 0 **The CVE Process**
- ➔ **Summary**

SANS Institute 2001 Top Ten uses CVE names …another step down the policy road



2. Vulnerable CGI programs and application extensions (e.g., ColdFusion) installed on web servers.

Most web servers support Common Gateway Interface (CGI) programs to provide interactivity in web pages, such as data collection and verification. Many web servers come with sample CGI programs installed by default. Unfortunately, many CGI programmers fail to consider ways in which their programs may be misused or subverted to execute malicious commands. Vulnerable CGI programs present a particularly attractive target to intruders because they are relatively easy to locate, and they operate with the privileges and power of the web server software itself. Intruders are known to have exploited vulnerable CGI programs to vandalize web pages, steal credit card information, and set up back doors to enable future intrusions, even if the CGI programs are secured. When Janet Reno's picture was replaced by that of Adolph Hitler at the Department of Justice web site, an in-depth assessment concluded that a CGI hole was the most probable avenue of compromise. Allaire's ColdFusion is a web server application package which includes vulnerable sample programs when installed. As a general rule, sample programs should always be removed from production systems.

Systems Affected:
All web servers.

CVE Entries:
** Sample CGI programs (All CGI)
Remedy:
Remove all sample CGI programs on a production server.

** CAN-1999-0736(IIS 4.0, Microsoft Site Server 3.0, which is included with Microsoft Site Server 3.0 Commerce Edition, Microsoft Commercial Internet System 2.0, and Microsoft BackOffice Server 4.0 and 4.5)

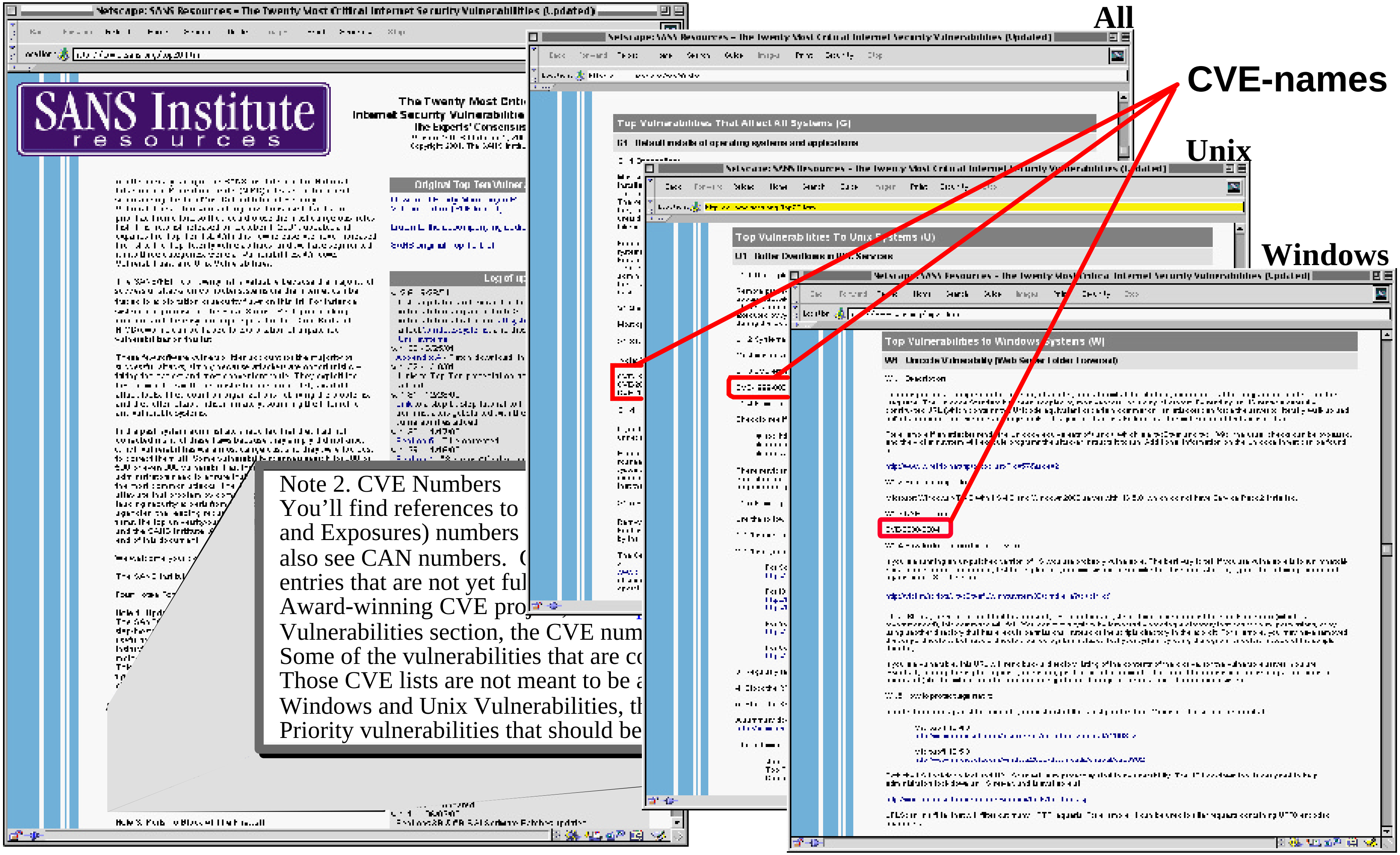
(see http://www.microsoft.com/technet/security/bulletin/ms99-013.asp)
Remedy:
Apply patch at : ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/usa/Viewcode-fix/

CVE-1999-0067 (phf phone book program included with older NCSA and Apache server)
CVE-1999-0068 ('mylog.html' sample script shipped with the PHP/FI)
CVE-1999-0270 (IRIX 6.2, IRIX 6.3, IRIX 6.4)
CVE-1999-0346 (sample script shipped with the PHP/FI package)
CVE-2000-0207 (IRIX 6.5)

CVE-names

http://www.sans.org/topten.htm

FBI/SANS Institute 2001 Top Twenty uses CVE names …yet another step down the policy road



Netscape: SANS Resources – The Twenty Most Critical Internet Security Vulnerabilities (Updated)

SANS Institute resources

The Twenty Most Criti
Internet Security Vulnerabilitie
The Experts' Consensus

Original Top Ten Vulner

Log of up

Note 2. CVE Numbers
You'll find references to
and Exposures) numbers
also see CAN numbers. (
entries that are not yet ful
Award-winning CVE pro
Vulnerabilities section, the CVE num
Some of the vulnerabilities that are co
Those CVE lists are not meant to be a
Windows and Unix Vulnerabilities, th
Priority vulnerabilities that should be

Top Vulnerabilities That Affect All Systems (G)

G1 Default installs of operating systems and applications

Top Vulnerabilities To Unix Systems (U)

U1 Buffer Overflows in RPC Services

Top Vulnerabilities to Windows Systems (W)

W1 Unicode Vulnerability (Web Server Folder Traversal)

All

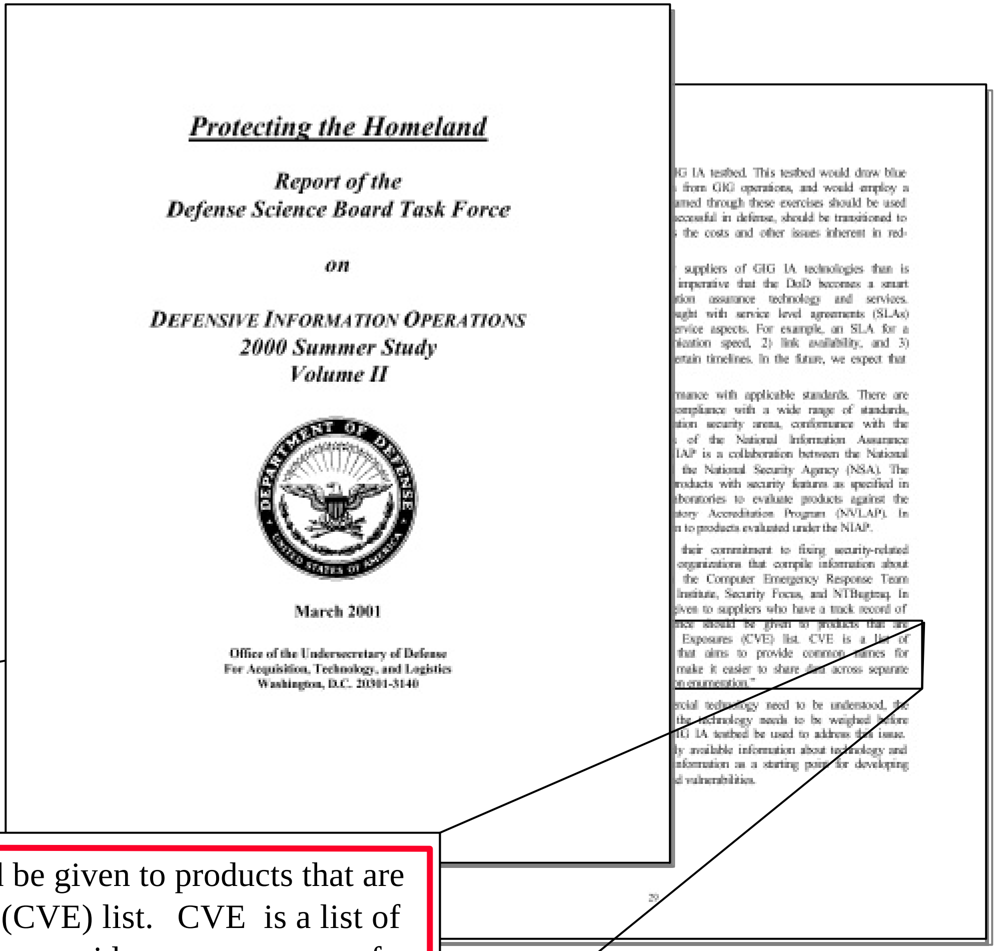
CVE-names

Unix

Windows

http://www.sans.org/top20.htm

Defense Science Board Report on Defensive Information Operations calls for CVE-compatible Products



Protecting the Homeland

Report of the
Defense Science Board Task Force

on

DEFENSIVE INFORMATION OPERATIONS
2000 Summer Study
Volume II

March 2001

Office of the Undersecretary of Defense
For Acquisition, Technology, and Logistics
Washington, D.C. 20301-3140

IG IA testbed. This testbed would draw blue
from GIG operations, and would employ a
arned through these exercises should be used
ccessful in defense, should be transitioned to
the costs and other issues inherent in red-

suppliers of GIG IA technologies than is
imperative that the DoD becomes a smart
tion assurance technology and services.
ught with service level agreements (SLAs)
ervice aspects. For example, an SLA for a
nication speed, 2) link availability, and 3)
ertain timelines. In the future, we expect that

rmance with applicable standards. There are
compliance with a wide range of standards,
ation security arena, conformance with the
of the National Information Assurance
IAP is a collaboration between the National
the National Security Agency (NSA). The
roducts with security features as specified in
boratories to evaluate products against the
tory Accreditation Program (NVLAP). In
n to products evaluated under the NIAP.

their commitment to fixing security-related
organizations that compile information about
the Computer Emergency Response Team
Institute, Security Focus, and NTBugtraq. In
given to suppliers who have a track record of
ence should be given to products that are
Exposures (CVE) list. CVE is a list of
that aims to provide common names for
make it easier to share data across separate
on enumeration."

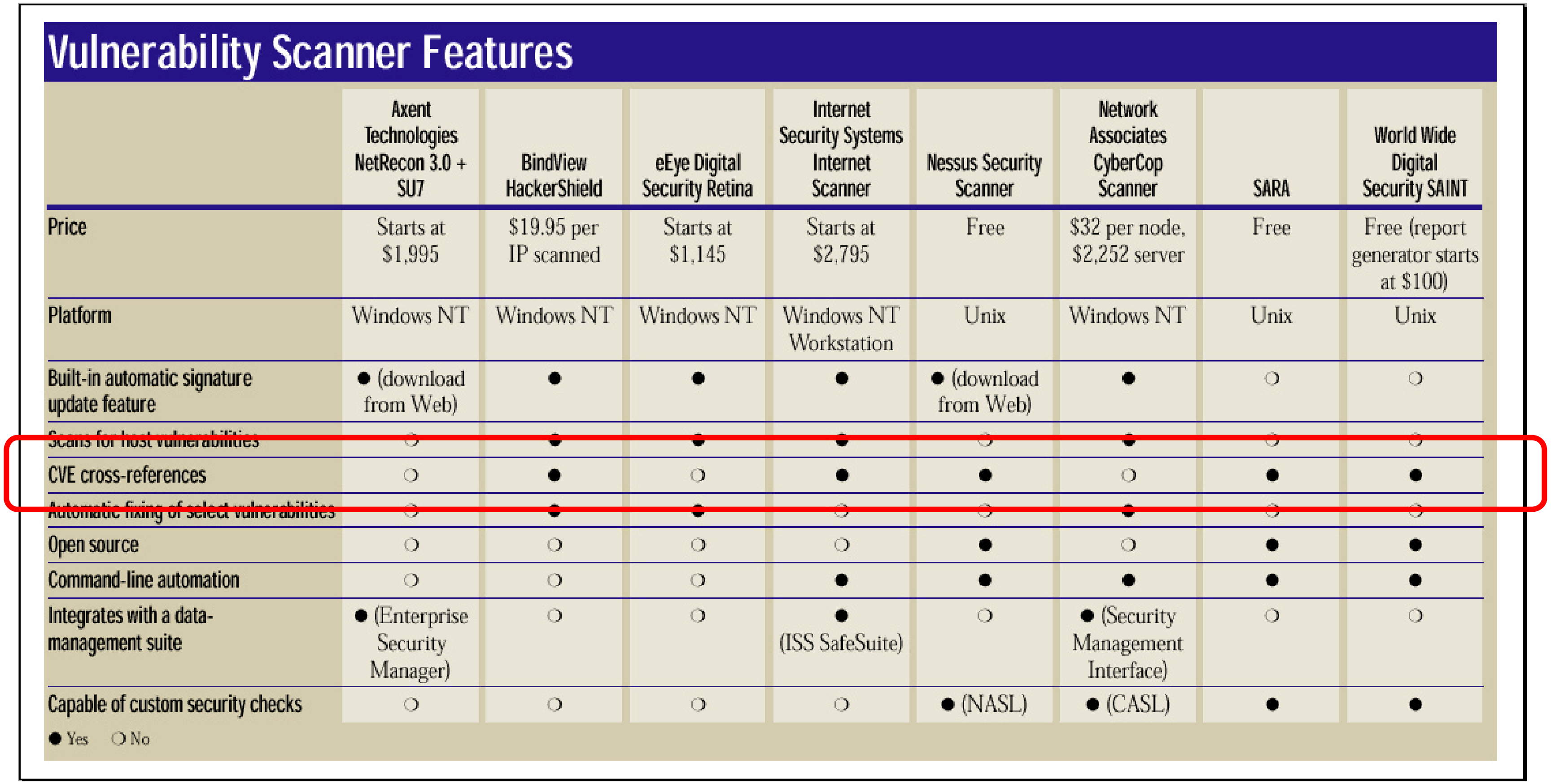
ercial technology need to be understood, the
the technology needs to be weighed before
IG IA testbed be used to address this issue.
ly available information about technology and
information as a starting point for developing
d vulnerabilities.

29

Furthermore, preference should be given to products that are Compatible with the Common Vulnerabilities and Exposures (CVE) list. CVE is a list of Information security vulnerabilities and exposures that aims to provide common names for Publicly known problems. The goal of CVE is to make it easier to share data across separate Vulnerability databases and security tools with a "common enumeration."

http://www.acq.osd.mil/dsb/tfreports.htm

CVE Has Become Part of Product Comparisons…a step down the road of policy...



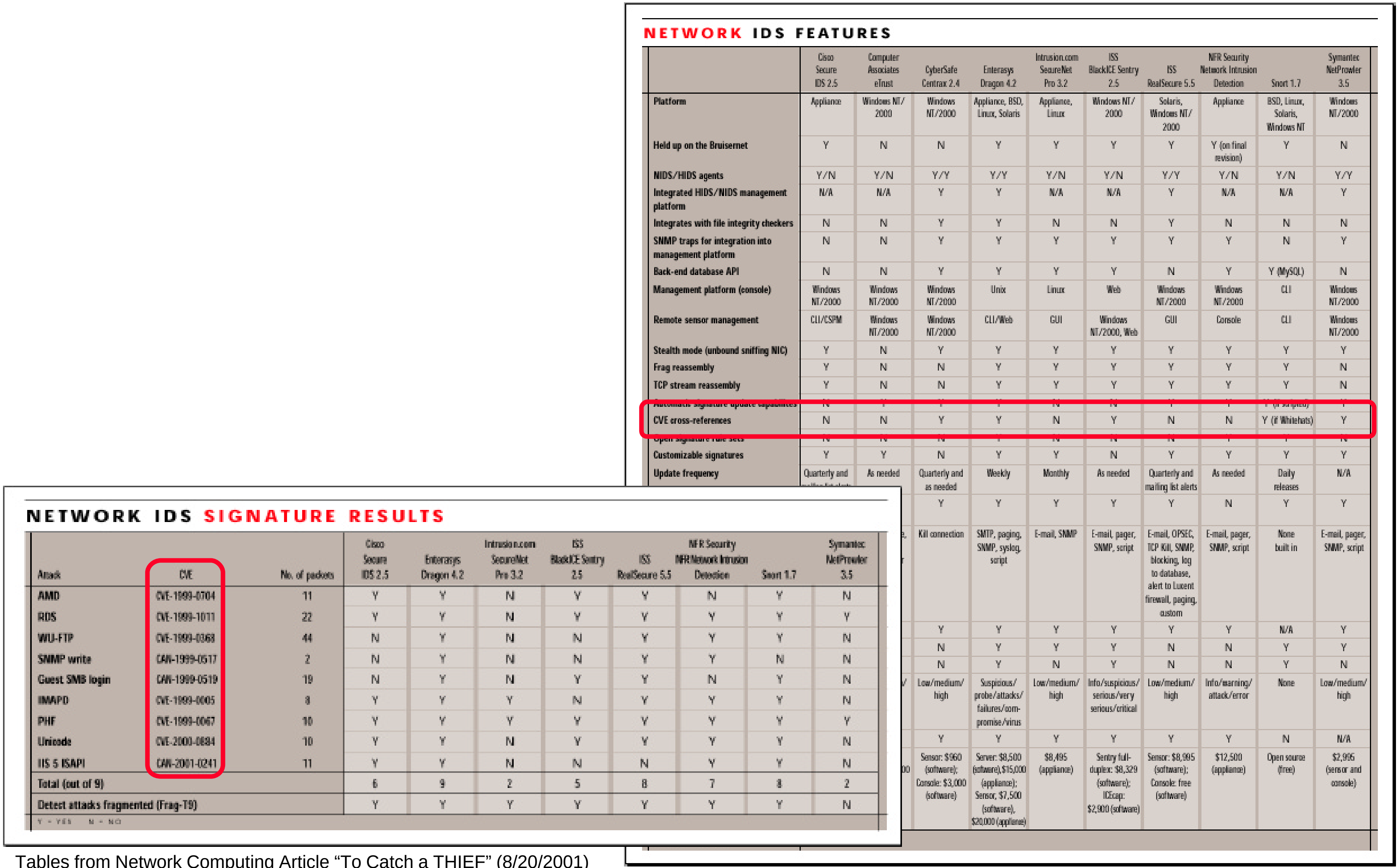
Vulnerability Scanner Features

	Axent Technologies NetRecon 3.0 + SU7	BindView HackerShield	eEye Digital Security Retina	Internet Security Systems Internet Scanner	Nessus Security Scanner	Network Associates CyberCop Scanner	SARA	World Wide Digital Security SAINT
Price	Starts at $1,995	$19.95 per IP scanned	Starts at $1,145	Starts at $2,795	Free	$32 per node, $2,252 server	Free	Free (report generator starts at $100)
Platform	Windows NT	Windows NT	Windows NT	Windows NT Workstation	Unix	Windows NT	Unix	Unix
Built-in automatic signature update feature	● (download from Web)	●	●	●	● (download from Web)	●	○	○
Scans for host vulnerabilities	○	●	●	●	○	●	○	○
CVE cross-references	○	●	○	●	●	○	●	●
Automatic fixing of select vulnerabilities	○	●	●	○	○	●	○	○
Open source	○	○	○	○	●	○	●	●
Command-line automation	○	○	○	●	●	●	●	●
Integrates with a data-management suite	● (Enterprise Security Manager)	○	○	● (ISS SafeSuite)	○	● (Security Management Interface)	○	○
Capable of custom security checks	○	○	○	○	● (NASL)	● (CASL)	●	●

● Yes ○ No

Network Computing Article “Vulnerability Assessment Scanners” (1/8/2001)

CVE Enables Detailed Product Comparisons



NETWORK IDS FEATURES

	Cisco Secure IDS 2.5	Computer Associates eTrust	CyberSafe Centrax 2.4	Enterasys Dragon 4.2	Intrusion.com SecureNet Pro 3.2	ISS BlackICE Sentry 2.5	ISS RealSecure 5.5	NFR Security Network Intrusion Detection	Snort 1.7	Symantec NetProwler 3.5
Platform	Appliance	Windows NT/ 2000	Windows NT/2000	Appliance, BSD, Linux, Solaris	Appliance, Linux	Windows NT/ 2000	Solaris, Windows NT/ 2000	Appliance	BSD, Linux, Solaris, Windows NT	Windows NT/2000
Held up on the Bruisernet	Y	N	N	Y	Y	Y	Y	Y (on final revision)	Y	N
NIDS/HIDS agents	Y/N	Y/N	Y/Y	Y/Y	Y/N	Y/N	Y/Y	Y/N	Y/N	Y/Y
Integrated HIDS/NIDS management platform	N/A	N/A	Y	Y	N/A	N/A	Y	N/A	N/A	Y
Integrates with file integrity checkers	N	N	Y	Y	N	N	Y	N	N	N
SNMP traps for integration into management platform	N	N	Y	Y	Y	Y	Y	Y	N	Y
Back-end database API	N	N	Y	Y	Y	Y	N	Y	Y (MySQL)	N
Management platform (console)	Windows NT/2000	Windows NT/2000	Windows NT/2000	Unix	Linux	Web	Windows NT/2000	Windows NT/2000	CLI	Windows NT/2000
Remote sensor management	CLI/CSPM	Windows NT/2000	Windows NT/2000	CLI/Web	GUI	Windows NT/2000, Web	GUI	Console	CLI	Windows NT/2000
Stealth mode (unbound sniffing NIC)	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Frag reassembly	Y	N	N	Y	Y	Y	Y	Y	Y	N
TCP stream reassembly	Y	N	N	Y	Y	Y	Y	Y	Y	N
Automatic signature update capabilities	N	Y	Y	Y	N	N	Y	Y	Y (if scripted)	Y
CVE cross-references	N	N	Y	Y	N	Y	N	N	Y (if Whitehats)	Y
Open signature rule sets	N	N	N	Y	N	N	N	Y	Y	N
Customizable signatures	Y	Y	N	Y	Y	N	Y	Y	Y	Y
Update frequency	Quarterly and mailing list alerts	As needed	Quarterly and as needed	Weekly	Monthly	As needed	Quarterly and mailing list alerts	As needed	Daily releases	N/A
			Y	Y	Y	Y	Y	N	Y	Y
			Kill connection	SMTP, paging, SNMP, syslog, script	E-mail, SNMP	E-mail, pager, SNMP, script	E-mail, OPSEC, TCP Kill, SNMP, blocking, log to database, alert to Lucent firewall, paging, custom	E-mail, pager, SNMP, script	None built in	E-mail, pager, SNMP, script
			Y	Y	Y	Y	Y	Y	N/A	Y
			N	Y	Y	Y	N	N	Y	Y
			N	Y	N	Y	N	N	Y	N
			Low/medium/ high	Suspicious/ probe/attacks/ failures/com- promise/virus	Low/medium/ high	Info/suspicious/ serious/very serious/critical	Low/medium/ high	Info/warning/ attack/error	None	Low/medium/ high
			Y	Y	Y	Y	Y	Y	N	N/A
			Sensor: $960 (software); Console: $3,000 (software)	Server: $8,500 (software), $15,000 (appliance); Sensor, $7,500 (software), $20,000 (appliane)	$8,495 (appliance)	Sentry full-duplex: $8,329 (software); ICEcap: $2,900 (software)	Sensor: $8,995 (software); Console: free (software)	$12,500 (appliance)	Open source (free)	$2,995 (sensor and console)

NETWORK IDS SIGNATURE RESULTS

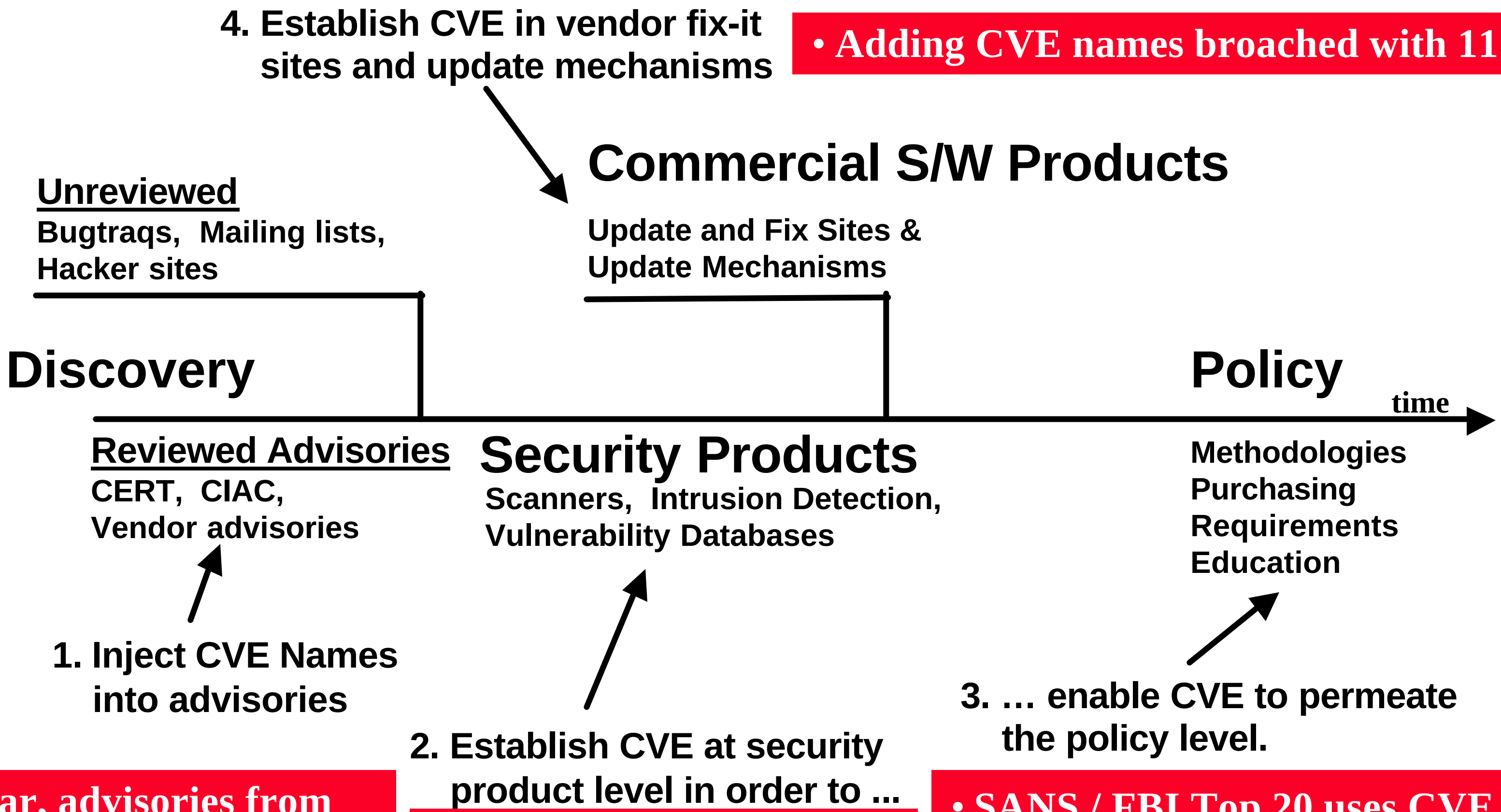
Attack	CVE	No. of packets	Cisco Secure IDS 2.5	Enterasys Dragon 4.2	Intrusion.com SecureNet Pro 3.2	ISS BlackICE Sentry 2.5	ISS RealSecure 5.5	NFR Security NFR Network Intrusion Detection	Snort 1.7	Symantec NetProwler 3.5
AMD	CVE-1999-0704	11	Y	Y	N	Y	Y	N	Y	N
RDS	CVE-1999-1011	22	Y	Y	N	Y	Y	Y	Y	Y
WU-FTP	CVE-1999-0368	44	N	Y	N	N	Y	Y	Y	N
SNMP write	CAN-1999-0517	2	N	Y	N	N	Y	Y	N	N
Guest SMB login	CAN-1999-0519	19	N	Y	N	Y	Y	N	Y	N
IMAPD	CVE-1999-0005	8	Y	Y	Y	N	Y	Y	Y	N
PHF	CVE-1999-0067	10	Y	Y	Y	Y	Y	Y	Y	Y
Unicode	CVE-2000-0884	10	Y	Y	N	Y	Y	Y	Y	N
IIS 5 ISAPI	CAN-2001-0241	11	Y	Y	N	N	N	Y	Y	N
Total (out of 9)			6	9	2	5	8	7	8	2
Detect attacks fragmented (Frag-T9)			Y	Y	Y	Y	Y	Y	Y	N

Y = YES N = NO

Tables from Network Computing Article “To Catch a THIEF” (8/20/2001)

The CVE Strategy: Where are we? (as of 17 October 2001)

- Adding CVE names broached with 11 groups.



4. Establish CVE in vendor fix-it sites and update mechanisms

Commercial S/W Products

Update and Fix Sites &
Update Mechanisms

Unreviewed
Bugtraqs, Mailing lists,
Hacker sites

Discovery

Policy

Reviewed Advisories
CERT, CIAC,
Vendor advisories

Security Products

Scanners, Intrusion Detection,
Vulnerability Databases

Methodologies
Purchasing
Requirements
Education

1. Inject CVE Names into advisories

2. Establish CVE at security product level in order to ...

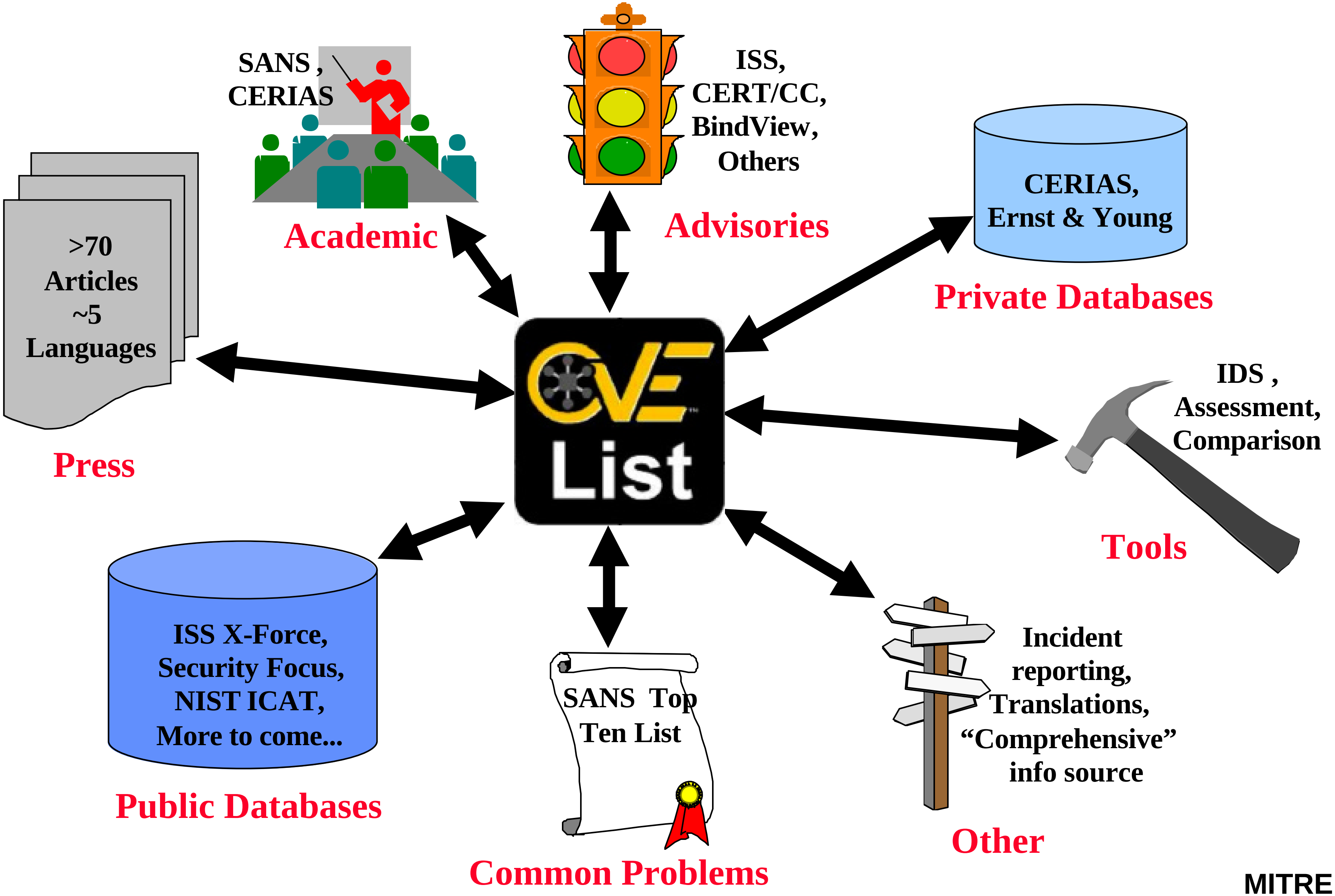
3. … enable CVE to permeate the policy level.

So far, advisories from ISS X-Force, Rain Forest Puppy, BindView, Compaq, SGI, IBM, CERT/CC, Microsoft, HP, and CISCO have included CVE names.

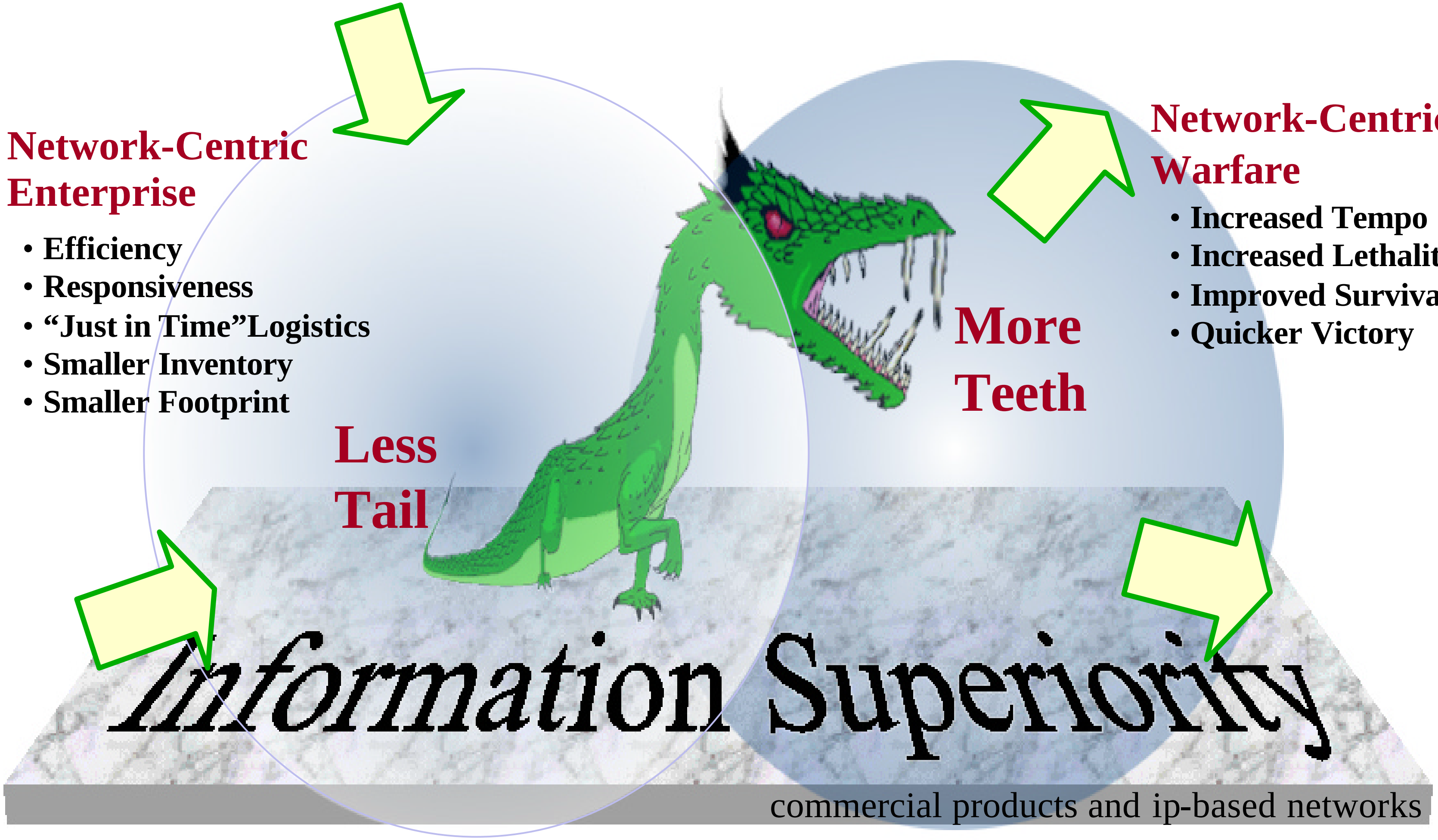
- 1604 CVE Entries -- 1880 Candidates.
- 64 CVE-compatible products from 39 groups.
- 14 more from 12 others in “the works”.

- SANS / FBI Top 20 uses CVE names
- Network Computing IDS & Scanner Comparisons included CVE
- DSB Report calls for CVE compatibility
- Network World IDS Comparison included CVE coverage

CVE is the center of many activities and efforts… …and it's still growing



CVE is helping make the critical task of effective vulnerability management possible



Network-Centric Enterprise

- Efficiency
- Responsiveness
- “Just in Time”Logistics
- Smaller Inventory
- Smaller Footprint

Less Tail

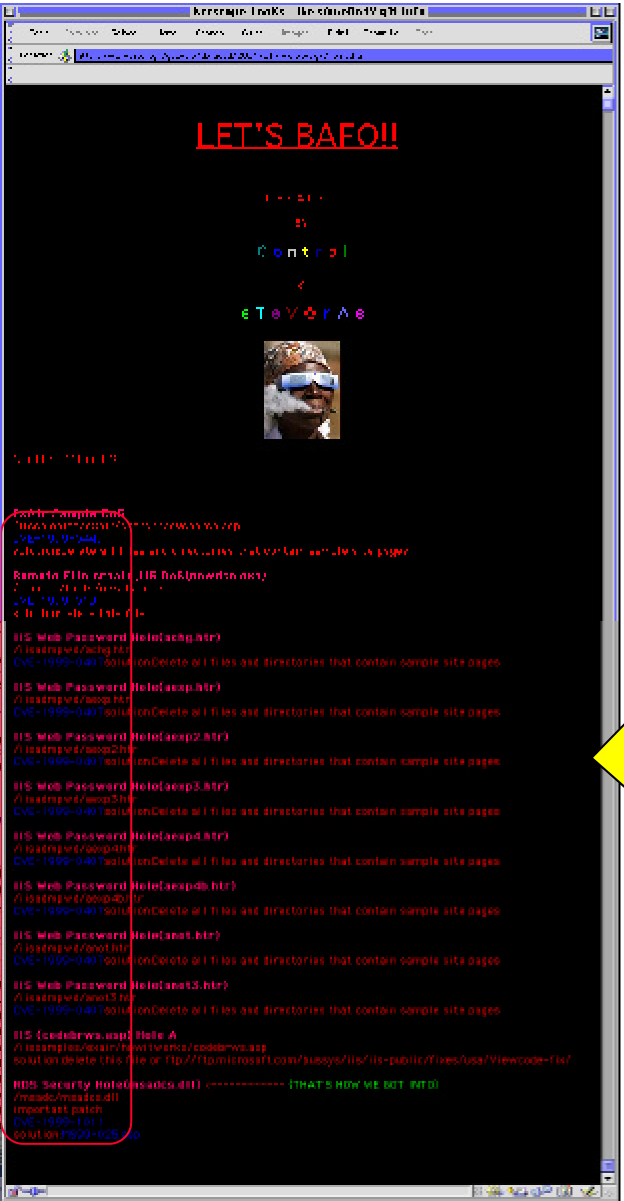
More Teeth

Network-Centric Warfare

- Increased Tempo
- Increased Lethality
- Improved Survivability
- Quicker Victory

Commercial-based network-centricism requires management of product vulnerabilities

CVE is even getting used by Hackers !



LET'S BAFO!!

[illegible]

Control

[illegible]

[illegible]

IIS Web Password Hole(achg.htr)
/iisadmpwd/achg.htr
CVE-1999-0407solutionDelete all files and directories that contain sample site pages

IIS Web Password Hole(aexp.htr)
/iisadmpwd/aexp.htr
CVE-1999-0407solutionDelete all files and directories that contain sample site pages

IIS Web Password Hole(aexp2.htr)
/iisadmpwd/aexp2.htr
CVE-1999-0407solutionDelete all files and directories that contain sample site pages

IIS Web Password Hole(aexp3.htr)
/iisadmpwd/aexp3.htr
CVE-1999-0407solutionDelete all files and directories that contain sample site pages

IIS Web Password Hole(aexp4.htr)
/iisadmpwd/aexp4.htr
CVE-1999-0407solutionDelete all files and directories that contain sample site pages

IIS Web Password Hole(aexp4b.htr)
/iisadmpwd/aexp4b.htr
CVE-1999-0407solutionDelete all files and directories that contain sample site pages

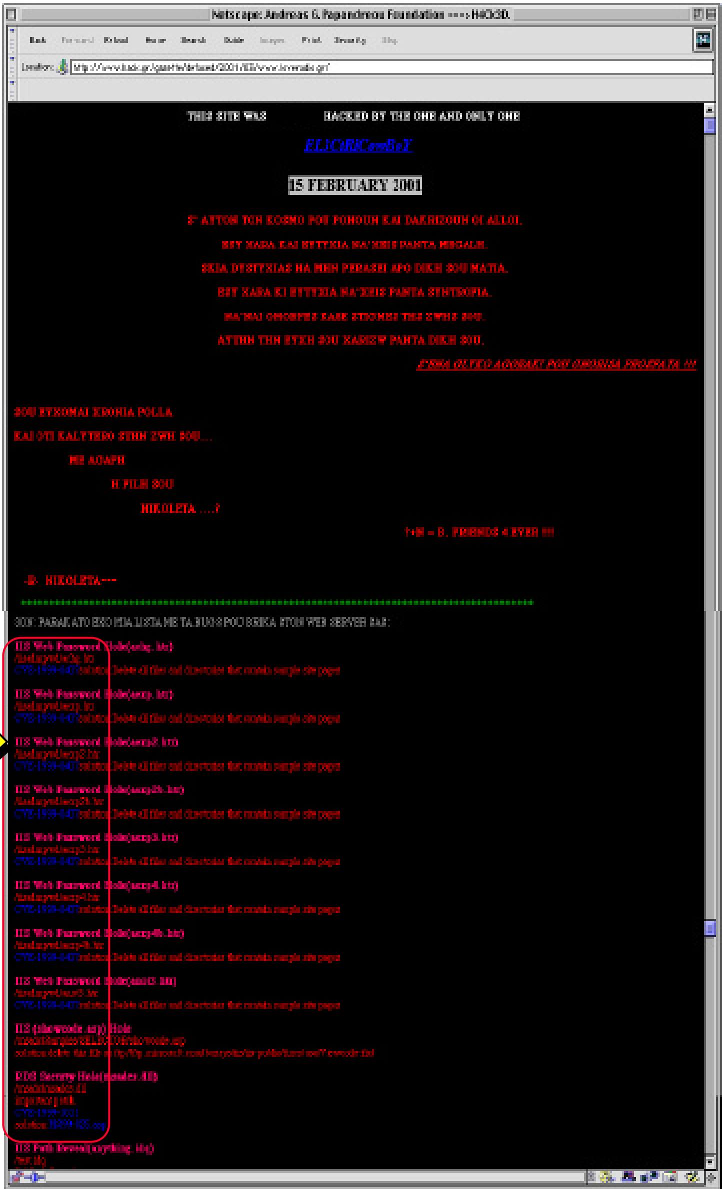
IIS Web Password Hole(anot.htr)
/iisadmpwd/anot.htr
CVE-1999-0407solutionDelete all files and directories that contain sample site pages

IIS Web Password Hole(anot3.htr)
/iisadmpwd/anot3.htr
CVE-1999-0407solutionDelete all files and directories that contain sample site pages

IIS (codebrws.asp) Hole A
/iissamples/exair/howitworks/codebrws.asp
solution:delete this file or ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/usa/Viewcode-fix/

RDS Security Hole(msadcs.dll) <------------ (THAT'S HOW WE GOT INTO)
/msadc/msadcs.dll
important patch
CVE-1999-1011
solution:MS99-025.asp

At least two hackers are now suppling CVE names for the vulnerabilities that they find in the sites they hack into.



Netscape: Andreas G. Papandreou Foundation ----> H4Ck3D.

Location: http://www.[illegible]/2001/02/www.[illegible].gr/

THIS SITE WAS HACKED BY THE ONE AND ONLY ONE

[illegible]

15 FEBRUARY 2001

S' AYTON TON KOSMO POY PONOUN KAI DAKRIZOUN OI ALLOI.

EYX XARA KAI EYTYXIA NA'XEIS PANTA MEGALH.

SKIA DYSTYXIAS NA MHN PERASEI APO DIKH SOU MATIA.

EYX XARA KI EYTYXIA NA'XEIS PANTA SYNTROFIA.

NA'NAI OMORFES SAN STIGMES TIS ZWHS SOU.

AYTHN THN EYXH SOU XARIZW PANTA DIKH SOU.

[illegible]

SOU EYXOMAI XRONIA POLLA

KAI OTI KALYTERO STHN ZWH SOU...

ME AGAPH

H FILH SOU

NIKOLETA ....?

[illegible] FRIENDS 4 EVER !!!

-D- NIKOLETA---

SOS: PARAKATO EXO MIA LISTA ME TA BUGS POU BRIKA STON WEB SERVER SAS :

IIS Web Password Hole(achg.htr)
/iisadmpwd/achg.htr
CVE-1999-0407solution:Delete all files and directories that contain sample site pages

IIS Web Password Hole(aexp.htr)
/iisadmpwd/aexp.htr
CVE-1999-0407solution:Delete all files and directories that contain sample site pages

IIS Web Password Hole(aexp2.htr)
/iisadmpwd/aexp2.htr
CVE-1999-0407solution:Delete all files and directories that contain sample site pages

IIS Web Password Hole(aexp2b.htr)
/iisadmpwd/aexp2b.htr
CVE-1999-0407solution:Delete all files and directories that contain sample site pages

IIS Web Password Hole(aexp3.htr)
/iisadmpwd/aexp3.htr
CVE-1999-0407solution:Delete all files and directories that contain sample site pages

IIS Web Password Hole(aexp4.htr)
/iisadmpwd/aexp4.htr
CVE-1999-0407solution:Delete all files and directories that contain sample site pages

IIS Web Password Hole(aexp4b.htr)
/iisadmpwd/aexp4b.htr
CVE-1999-0407solution:Delete all files and directories that contain sample site pages

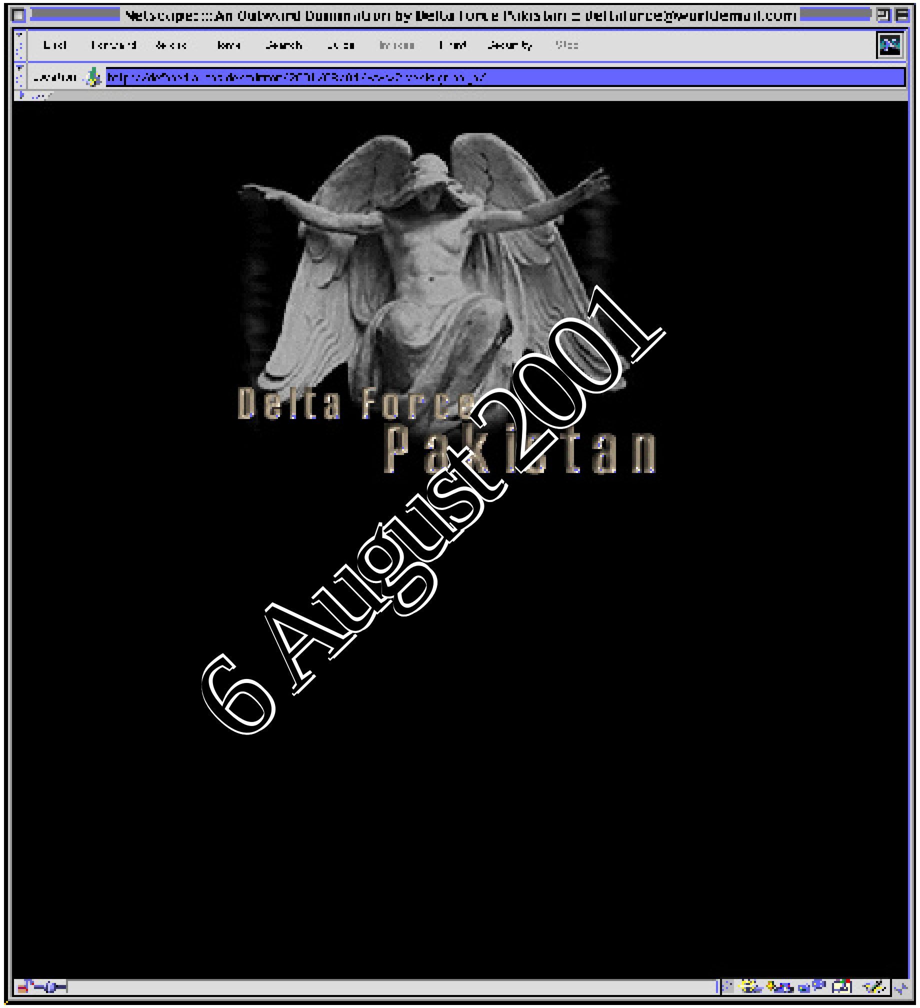
IIS Web Password Hole(anot3.htr)
/iisadmpwd/anot3.htr
CVE-1999-0407solution:Delete all files and directories that contain sample site pages

IIS (showcode.asp) Hole
/msadc/Samples/SELECTOR/showcode.asp
solution:delete this file or ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/usa/Viewcode-fix/

RDS Security Hole(msadcs.dll)
/msadc/msadcs.dll
important patch
CVE-1999-1011
solution:MS99-025.asp

IIS Path Reveal(anything.idq)
/test.idq

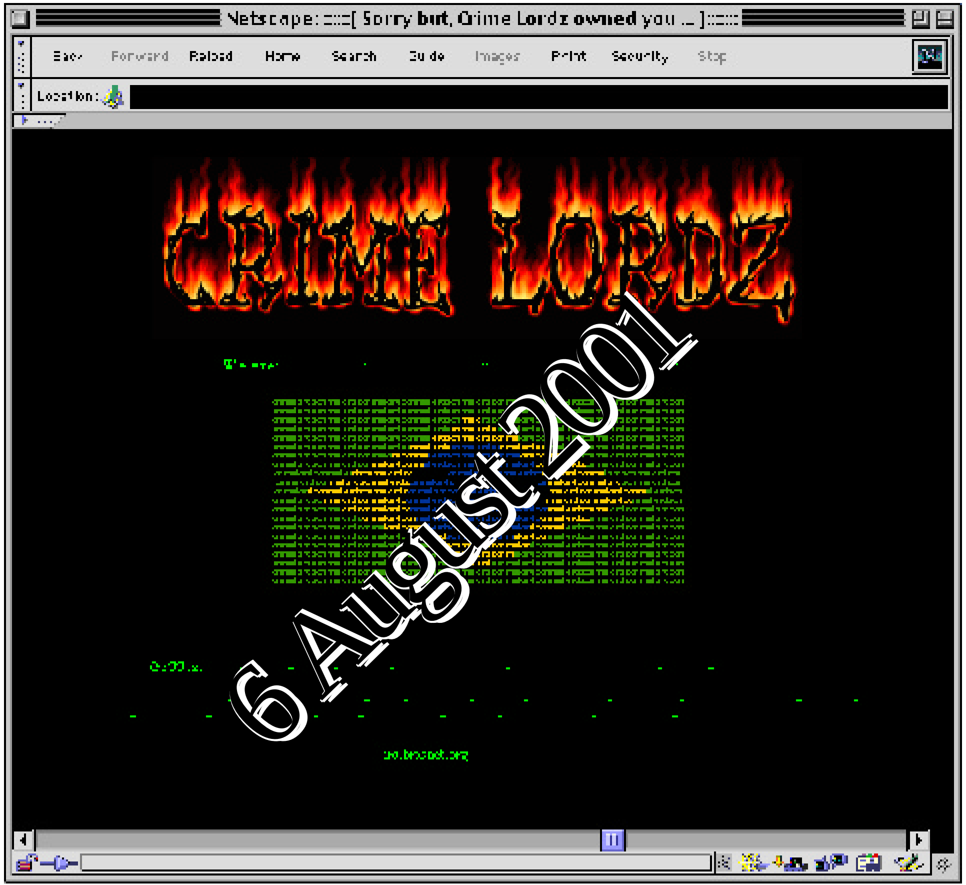
And Yes, In Case You Wondered… …the Hacking Continues


Netscape: :::An Outward Domination by Delta Force Pakistan = deltaforce@worldemail.com
Delta Force
Pakistan

6 August 2001

VeriSign Inc. Japanese Site
http://www.verisign.co.jp

Bureau of Land Management in California
http://www.ca.blm.gov



6 August 2001

For More Information

CVE web site

http://cve.mitre.org